Escuela Politécnica Superior

Desarrollo de un SGSI para un grupo empresarial

Máster Universitario en Ciberseguridad

Trabajo Fin de Máster

Autor:
Ignacio Piera Cebrián

Tutor/es:
José Vicente Berná Martínez

Junio 2021

Universitat d'Alacant
Universidad de Alicante

Resumen

Por mi experiencia profesional, la mayoría de las empresas pequeñas o medianas carecen de cualquier tipo de formalismo o plan de seguridad. En este proyecto se plantea formalizar el SGSI para un grupo empresarial donde convergen varios tipos de empresas diferentes, con necesidades diferentes, de un tamaño considerable en conjunto, pero que son administradas desde un servicio de TI unificado. Esta estructura empresarial particular requiere de un análisis y planificación concreta que se materializará en un Plan Director de Seguridad Empresarial.

Este Plan Director de la Seguridad Empresarial, abordará el estudio del contexto de la empresa, la evaluación de los niveles actuales de seguridad informática, comprobaran los puntos fuertes y los puntos débiles, para finalmente ofrecer un documento con propuestas y planes que puedan servir de ayuda a reforzar los mecanismos de seguridad informática del grupo empresarial.

Para ello se emplearan la familia de normativas ISO 27K, la Metodología Magerit v3 desarrollada por la Administración Electrónica del Gobierno de España y los planes de contingencia y continuidad de negocio desarrollados por el INCIBE.

Palabras clave: ciberseguridad, grupo empresarial, plan director de la seguridad informática, Magerit v3, ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, sistemas de gestión de la seguridad informática, planes de seguridad, plan de contingencia, plan de continuidad de negocio, estudio del contexto.

Motivación, justificación y objetivo general

Durante mi experiencia en el sector laboral como IT he comprobado de primera mano cómo la ciberseguridad es un aspecto muy poco tratado y desarrollado en el ámbito informático de las empresas. Ya sea por desconocimiento o por no darle la suficiente importancia, la ciberseguridad siempre se ha visto relegada a un segundo plano, como algo opcional o un gasto ineficiente de recursos. Aunque, en los últimos años y sobre todo desde el inicio de la pandemia mundial de la COVID-19, se han disparado el número de casos de ciberdelincuencia, lo que ha propiciado también la importancia de la ciberseguridad en toda clase de empresas y organismos.

Desde mi punto de vista, un Sistema de Gestión de la Seguridad de la Información, se presenta como un valioso aliado para la empresa u organización, ya que permite la organización y categorización de los activos, así como la evaluación de sus amenazas asociadas. Conociendo estas amenazas sobre los activos, podremos calcular los riesgos asociados y decidir si tomar medidas o no, con el desarrollo de los planes de seguridad orientados a reforzar las deficiencias de seguridad de los puntos más débiles del sistema.

Aprovechándome de la experiencia adquirida como IT en un grupo empresarial, deseo desarrollar la realización de un Plan Director de Seguridad orientado a un grupo de empresas que operan bajo la misma gerencia. Este grupo empresarial cuenta con ciertos mecanismos de seguridad ya implementados, por lo que deseo realizar un estudio para evaluar los niveles actuales de seguridad, comprobar los puntos fuertes y los puntos débiles, para finalmente ofrecer un documento con propuestas y planes que puedan servir de ayuda a reforzar los mecanismos de ciberseguridad del grupo empresarial.

Con este objetivo, emplearé mis conocimientos adquiridos en la asignatura “Sistemas de Gestión de la Seguridad” del Máster Universitario en Ciberseguridad en la Universidad de Alicante. Para ello, desarrollaré el Plan Director de Seguridad empleando la normativa ISO 27000, que es la norma establecida en España para la implementación de un Sistema de Gestión de Seguridad. Además, aplicaré varias recomendaciones y metodologías ofrecidas por el INCIBE, como la Magerit v3, para poder realizar una documentación estandarizada por la Administración Pública.

Pienso que el desarrollo de este Plan Director de Seguridad, me permitirá demostrar mis conocimientos adquiridos durante el Máster Universitario en Ciberseguridad, ya que estoy seguro de que va a poner a prueba todos mis conocimientos como Ingeniero, además de los adquiridos en el Máster.

Agradecimientos

En primer lugar, agradecer al grupo empresarial en el que me he basado para realizar este trabajo por la ayuda brindada. Además, a todo el personal del grupo empresarial por permitirme llevar a cabo esta investigación acerca de la seguridad informática de sus infraestructuras, por su paciencia y colaboración durante el desarrollo de este proyecto.

Agradezco especialmente a mi tutor del Trabajo de Final de Master, José Vicente Berná Martínez, por haberme permitido realizar este trabajo que ha sido de gran interés para mí y por haber sido tan atento conmigo siempre dispuesto a resolver cualquier duda que me ha surgido durante la realización de este proyecto.

Agradezco también a todos los profesores del máster por compartir sus conocimientos de una forma tan amena con nosotros y a mis compañeros de clase los cuales me han ayudado mucho y con los cuales he disfrutado de un año muy entretenido.

También quiero agradecer especialmente a mi hermano Juan Luis, por haberme dado la idea y motivación para realizar este master.

También quiero agradecer a mis amigos y mi familia por aguantarme durante tantos años y por su apoyo sin el cual no podría haber realizado este master.

Citas

Si tuviera la suerte de alcanzar alguno de mis ideales, sería en nombre de toda la humanidad.

Nikola Tesla

La ciencia, mi muchacho, está compuesta de errores, pero son errores que es útil cometer, porque conducen poco a poco a la verdad.

Julio Verne

Al mundo no le importará tu autoestima. El mundo esperará que logres algo, independientemente de que te sientas bien o no contigo mismo.

Bill Gates

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

Desde el inicio del nuevo milenio hasta nuestros días, las Tecnologías de la Información y Comunicación (TIC) se han extendido y adaptado en todos los ámbitos de la sociedad, ya sea para el ocio, la educación o para el ámbito empresarial, integrándose en nuestro día a día, con el propósito de simplificar los procesos y hacernos la vida más sencilla. Esto ha provocado que todos los datos que antiguamente se obtenían y procesaban de forma manual, actualmente sean obtenidos la mayoría de forma automática y gestionados de forma autónoma por las TIC.

Antiguamente, los datos de vital importancia a la hora de ser protegidos, eran almacenados en cajas de seguridad; pero actualmente, donde la mayoría de datos se conservan en formato digital, es necesario adaptar las empresas u organizaciones en el ámbito de la ciberseguridad con el objetivo de proteger estos datos ante cualquier posible agente malicioso que pueda poner en compromiso la seguridad de los datos.

Desde el punto de vista de la ciberseguridad, se considera necesario proteger los datos para que cumplan con los principios de integridad, confidencialidad e disponibilidad.

Asegurar la integridad de los datos, consiste en asegurar la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.

Asegurar la confidencialidad, consiste en garantizar que cierta información solo sea accesible por el personal autorizado a acceder a dichos datos.

Asegurar la disponibilidad, consiste en asegurar que unos datos puedan ser accesibles y utilizados por los usuarios o procesos autorizados cuando estos sean requeridos.

Al conseguir que la información pueda cumplir estos puntos, conseguiremos establecer un sistema donde la información tenga un grado alto de seguridad. Así pues, con el objetivo de asegurar la seguridad de los datos en una empresa u organización, necesitaremos realizar la implantación de un Sistema de Gestión de la Seguridad Informática (SGSI) donde: prestaremos atención a los activos de la empresa, evaluaremos a qué tipo de amenazas que puedan afectar a los principios mencionados anteriormente se podrán exponer y con ello, tomar las medidas que se crean oportunas para reducir el riesgo al que los activos pueden verse sometidos.

Para organizar el SGSI es necesario desarrollar un Plan Director de Seguridad (PDS), que a su vez se compone de un conjunto de proyectos mediante los cuales las decisiones adoptadas para el tratamiento y reducción de riesgos se materializan. El Plan Director incluye las prioridades, responsables, activos afectados y costes que implicarán cada uno de los planes. Además, incluye una planificación temporal estimada para poner todos los planes en marcha. Finalmente, este Plan de Seguridad, deberá ser aprobado por la organización contando con el compromiso de la dirección, si esta considera el plan adecuado con los objetivos estratégicos de la empresa.

En este trabajo se desarrollará un SGSI para un grupo empresarial compuesto de varias empresas dedicadas a la fabricación conformadas en diferentes sedes conectadas entre sí mediante redes de comunicación. Es un grupo empresarial basado en un grupo empresarial real, por lo que contaré con información de primera mano de los responsables de informática del grupo empresarial para poder realizar el desarrollo. Por motivos de seguridad, no usaré el nombre de la empresa ni mencionaré nombre de personas o localizaciones que puedan hacer referencia al grupo empresarial real. Tras desarrollar el SGSI, elaboraré una propuesta de Plan de Seguridad acorde a los objetivos de la empresa.

Este grupo empresarial, cuenta con información como puede tratarse de la actividad de negocio o información sensible como los datos personales de los proveedores, empleados y clientes, por lo que esta información tendrá que ser protegida con el objetivo de cumplir la Ley de Protección de Datos.

Para desarrollar el Plan Director de Seguridad, haremos uso de la norma ISO 27000 y de la metodología MAGERIT – versión 3.0 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) elaborada y avalada por el Consejo Superior de Administración Electrónica del Gobierno de España.

De acuerdo con este plan, comenzaremos con la obtención del catálogo de activos del grupo empresarial, para a partir de este catálogo comprobar las amenazas que más podrán poner en riesgo la seguridad y calcular los riesgos a los que se encuentran sometidos estos activos. A continuación, aplicaremos una serie de contramedidas, directrices y controles con el objetivo de rebajar el riesgo de estos activos, con el objetivo salvaguardar la información del sistema. Y finalmente, estableceremos las diferentes operaciones ordenadas según las prioridades establecidas en el Plan de Seguridad de la empresa que se pondrá a disposición de esta para su evaluación y si es aceptada, su futura implantación. El objetivo final, es la posibilidad de preparar la organización para la obtención de la certificación ISO 27001 en un futuro por parte de la empresa.

2. Estudio de viabilidad

Antes de comenzar a desarrollar el proyecto, es interesante considerar la realización de un estudio de viabilidad para analizar el proyecto en sí mismo y obtener una visión global de lo que nos puede aportar el proyecto y los costes que se deben asumir para conseguir llevarlo a buen puerto. Ya que el diseño de un SGSI puede llegar a implicar un alto coste presupuestario y de esfuerzo para una pequeña empresa, con el estudio de viabilidad podremos considerar si es rentable asumir el coste ante el posible beneficio.

Para realizar este estudio, emplearemos un análisis DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades), la cual es una metodología de estudio de la situación de un proyecto, analizando sus características internas (Debilidades y Fortalezas) y su situación externa (Amenazas y Oportunidades) en una matriz cuadrada como la que presentamos a continuación.

	Positivo	Negativo
Interno	Fortalezas: - Interés de la empresa por el refuerzo de la seguridad. - Alta implicación por parte de la dirección. - La empresa ya cuenta con ciertas medidas de seguridad que buscan ser reforzadas.	Debilidades: - Elevado coste del análisis del SGSI y de la certificación. - Personal con falta de formación en el campo de la informática y ciberseguridad. - Gran cantidad de activos obsoletos en materia de seguridad y necesarios para el día a día (maquinaria antigua).
Externo	Oportunidades: - Un SGSI ayuda a cumplir normativas legales referentes a la seguridad de la información. - Una empresa con una certificación en ciberseguridad inspira confianza en aquellos clientes que teman por la vulnerabilidad de sus datos.	Amenazas: - Se requiere una constante renovación de los Planes de Seguridad. - Existen empresas con mucha experiencia en el desarrollo de SGSI y Planes de Seguridad.

Figura 1. Análisis DAFO

3. Planificación

El plan original es realizar la presentación de este TFM en la convocatoria de Junio, por lo tanto y para dar tiempo a mi tutor a estudiar y aceptar este trabajo con tiempo, debo tenerlo finalizado aproximadamente a comienzos del mes de Mayo.

A continuación, se muestra la planificación estimada del desarrollo del SGSI, el Plan Director de Seguridad y el desarrollo de este documento.

Tabla 1. Planificación temporal TFM

Contenidos	**Tiempo total**	**Fecha límite fin**
Motivación, justificación, objetivo general, Introducción	2 semanas	22 enero
Estudio de viabilidad y planificación	1 semana	29 enero
Estado del arte	2 semanas	12 febrero
Objetivos	1 semana	19 febrero
Entrevistas con la empresa	1 semana	26 febrero
Metodología Análisis y especificación Presupuesto, estimaciones	2 semanas	5 marzo
Diseño SGSI	2 semanas	19 marzo
Implementación SGSI	1 mes	16 abril
Resultados Conclusiones y trabajo futuro Referencias, bibliografía y apéndices Agradecimientos, citas, índices	2 semanas	1 mayo
Envío del TFM		1 mayo
Defensa TFM		junio

4. Estado del arte.

En este capítulo se describe el contexto en el que se centra este trabajo. Se explicará el contexto del grupo empresarial, así como de los Sistemas de Gestión de Seguridad de la Información, la familia de normas ISO 27000 en la que nos basaremos, la metodología MAGERIT y el Plan Director de Seguridad.

4.1. Seguridad en grupos empresariales.

Un grupo empresarial cuenta con una gran cantidad de información generada por la propia empresa y sus clientes o proveedores, de gran valor que debe ser protegida por el propio bien hacer de la organización, tanto como para evitar problemas legales o evitar filtraciones de información. Tal y como se indica en la guía de INCIBE sobre Ciberamenazas contra entornos empresariales: una guía de aproximación para el empresario [1] (en la página 9):

"Cualquier empresa, ya sea una gran corporación o una pequeña pyme, gestiona información de gran valor no solo para la propia empresa, sino también para los ciberdelincuentes. Además, no solamente la información es el objetivo de los ciberdelincuentes, los sistemas que la gestionan también son de su interés ya que pueden ser utilizados para perpetrar nuevos fraudes o simplemente para extorsionar a la empresa propietaria."

Queda claro que es necesario proteger la información y los sistemas del grupo empresarial. Pero la ciberseguridad no se limita únicamente a proteger la organización de las amenazas que ponen en riesgo los sistemas informáticos o la información.

Tal y como se explica en el Decálogo ciberseguridad empresas de INCIBE [2] (en las páginas 6-8), también es necesario tener en cuenta la seguridad legal, que es aquella que garantiza el cumplimiento de todas las normativas y leyes que afecten a nuestros sistemas de información, con el objetivo de cumplir con las obligaciones legales y mejorar la reputación de la organización.

Este tipo de seguridad hace referencia a:

- Las normativas legales que toda empresa debe cumplir. Leyes aplicables a toda empresa que opere en territorio nacional y relacionadas con la gestión y protección de la información de usuarios y clientes, así como los sistemas informáticos que la tratan. Siendo las principales:

    - Ley Orgánica de Protección de Datos (LOPD) [3]
    - Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) [4]
    - Ley de Propiedad Intelectual (LPI) [5]
- La Seguridad con terceros. Al contratar servicios externos se tendrá que acordar con los proveedores los niveles del servicio (SLA) que nos prestan, mediante contratos, firmados por escrito, donde se establezcan los niveles de calidad del servicio, estableciendo penalizaciones en caso de incumplimiento.
- Seguridad interna con los empleados. Es necesario elaborar unos acuerdos de confidencialidad que los empleados tendrán que aceptar y firmar, con los que se regularan aspectos relativos a la prestación del servicio, incluyendo las sanciones en caso de incumplimiento.

¿Pero cómo se puede organizar la seguridad de la información y de la infraestructura en un grupo empresarial? Organismos internacionales como la Cámara de Comercio Internacional (ICC), nos aportan guías para establecer mecanismos de seguridad en nuestros empresariales. Según la Guía de Ciberseguridad para negocios del ICC [6] (en la página 5), se marcan tres puntos clave para un buen programa de seguridad:

- Por parte de la gestión empresarial, se debe realizar un análisis de riesgos para su organización y poder priorizar aquellos que requieran de una mayor protección.
- Se requiere liderazgo para tomar las medidas organizativas necesarias que garanticen las mejores prácticas de seguridad de la información.
- La empresa debe de estar preparada para detectar y responder, tanto de forma interna como externa, a las amenazas cibernéticas a través de una organización institucionalizada.

Por ello, queda claro que es necesario establecer un Sistema de Gestión de la Seguridad Informática para permitir a la empresa establecer unos planes de seguridad con el objetivo de protegerla ante los riesgos de las tecnologías de la información.

4.2. Sistemas de Gestión de la Seguridad Informática.

Un Sistema de la Gestión de la Seguridad Informática (SGSI) está formado por una serie de políticas, procesos, guías y recursos destinados a organizar y actuar sobre todos los elementos que componen la seguridad de una organización con el objetivo de garantizar la seguridad de la información. Un SGSI permite a una organización establecer el diseño, implantación, monitorización y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información reduciendo en todo lo posible los riesgos de seguridad de la información. [7] (en las páginas 11-12)

De acuerdo con la Norma ISO/IEC 27000 [7] (en la página 13), se destaca la importancia del SGSI por la necesidad de proteger la información de la empresa u organización (públicas o privadas) de las amenazas a las que se encuentran expuestas en las redes, sistemas y procesos que tratan con esa información. Pudiéndose tratar de riesgos internos o externos, como ataques de fraude, espionaje, sabotaje, vandalismo, fuego… o ataques más sofisticados como código malicioso, denegación de servicio, hackeos, ect.

La adopción de un SGSI se presenta como una decisión estratégica para una organización y es necesario que esta sea integrada, escalada y actualizada según las necesidades de todas las partes interesadas de la organización. Dicho así, requiere además del compromiso de los departamentos involucrados, la gerencia y los departamentos de IT, ya que muchas veces las soluciones de seguridad técnicas requieren además de cambios en la administración.

La adopción exitosa de un SGSI por parte de una organización, además de asegurar la información, le permitirá: lograr una mayor seguridad de que sus activos de información están adecuadamente protegidos contra amenazas de forma continua, mantener un marco estructurado y completo para identificar y evaluar los riesgos de seguridad de la información, seleccionando y aplicando los controles aplicables para medir y mejorar su efectividad, mejorar continuamente su entorno de control y asegurarse el cumplimiento de las normativas legales [7] (en las páginas 13-14).

En el territorio español contamos con la norma de la familia ISO/IEC publicada como UNE-ISO/IEC 27000. Se encuentra publicada por AENOR (Organismo de Normalización de España) y la última versión disponible es la del año 2019, quedando la del año 2014 y anteriores como anuladas. En la elaboración de este TFM, emplearé la norma ISO/IEC 27000 del año 2018.

4.3. Normativa ISO 27000.

La familia de normas ISO/IEC 27000 están dirigidas al desarrollo, implantación y operación de un Sistema de Gestión de la Seguridad de la Información, se incluyen bajo el título de "Tecnología de la información. Técnicas de seguridad".

La norma marca, que para establecer, monitorizar, mantener y mejorar un SGSI es necesario desarrollar los siguientes pasos, tal y como se redacta en el capítulo 4.5 “Estableciendo, monitorizando, manteniendo y mejorando un SGSI” [7] (Páginas 14-17):

1. Identificar los activos de información y sus correspondientes requisitos de seguridad.

2. Apreciar los riesgos de seguridad de información y tratar los riesgos de seguridad.

3. Seleccionar e implementar los controles pertinentes para gestionar los riesgos inaceptables.

4. Supervisar, mantener y mejorar la eficacia de los controles de seguridad asociados con los activos de información de la organización.

Tras la implantación de los controles, la organización tiene el deber de revisar los resultados y de evaluar si se han cambiado algunos de los aspectos que afectan a la seguridad y si la eficacia sigue siendo la adecuada. El Plan de Seguridad requerirá que se establezcan acciones continuas de análisis y evaluación de la situación actual, establecer objetivos de mejora y soluciones, evaluación de las soluciones y su implementación, medición y verificación de cumplimiento y formalizar los cambios en la correspondiente documentación de soporte.

Para contemplar una implantación exitosa de un SGSI es necesario que los intereses de la organización no estén enfrentados contra los objetivos de la organización, que los costes y necesidades del SGSI no causarán impacto sobre los procesos de negocio y que toda la empresa, desde los niveles directivos hasta los operativos e incluso partes externas, entiendan la necesidad de incluir la seguridad como un elemento no solo necesario sino de valor.

Para lograrlo, la familia ISO 27000 ayuda directamente a lograr la implantación de un SGSI en una empresa de forma alineada con la organización, ayudando a la dirección a estructurar la gestión de la seguridad dentro del gobierno corporativo, promover buenas prácticas de seguridad aceptadas a nivel mundial, establecer un vocabulario común (por eso de la definición de terminología inicial), aumentar la confianza en la organización, satisfacer las expectativas y necesidades y a obtener una gestión más eficaz de la seguridad de la información.

Para el presente trabajo he usado como base las siguientes normas [8] pertenecientes a la familia de normas ISO/IEC 27000, ya que esta norma es reconocida internacionalmente y utilizada como marco de referencia de herramientas de análisis y seguimiento.

- Norma ISO/IEC 27000 Sistemas de Gestión de Seguridad de la Información (SGSI). Visión de conjunto y vocabulario: describe los fundamentos de los SGSI sobre los que se constituye la familia ISO 27000 y define los términos relacionados.
- Norma ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos: especifica los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar los SGSI.
- Norma ISO/IEC 27002 Código de práctica para los controles de seguridad de la información: proporciona una lista de objetivos de control comúnmente aceptados así como las mejores prácticas en controles de seguridad que deben utilizarse como guía de aplicación para su selección e implementación para lograr la seguridad de la información.

4.4. Metodología Magerit.

La metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el CSAE (Consejo Superior de Administración Electrónica), fue diseñada siguiendo la terminología de la ISO 31000 con el objetivo de implementar el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información [9] (en la página 7).

MAGERIT permite calcular el valor de los activos una organización, las amenazas a los que estos activos están sometidos con el análisis del riesgo que ello conlleva y obtener ayuda a la hora de protegerlos. Con MAGERIT se busca una aproximación metódica, con el objetivo de cubrir todo ámbito y evitar dejar lugar a la improvisación ante un mismo análisis de valor, siempre teniendo en cuenta las principales dimensiones y subdimensiones de la seguridad: Integridad, Disponibilidad, Confidencialidad, Autenticidad y Trazabilidad

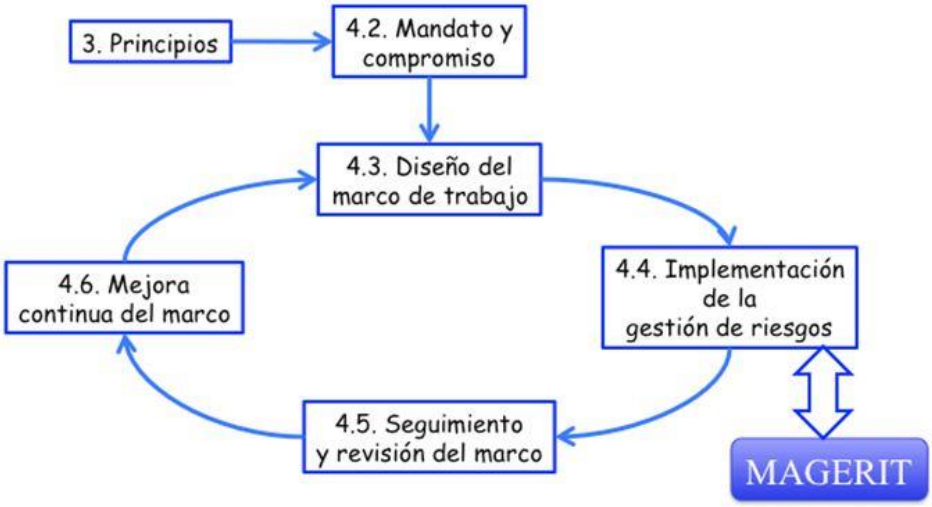


Figura 2. ISO 31000 - Marco de trabajo para la gestión de riesgos (Fuente MAGERIT v3 – Libro I)

Dentro de la gestión de riesgos, existen varias metodologías además de MAGERIT v3, como pueden ser: EBIOS, CRAMM, MEHARI, NIST SP 800-30, Octave, SP800-30.

Para la abordar la gestión de riesgos desarrollada en este TFM, usaremos la versión 3 de la metodología publicada en el año 2012, por ser de las más utilizadas en España para el desarrollo de SGSI y por tener ya experiencia con ella. Esta metodología se encuentra disponible de forma gratuita para su uso en el Portal de la Administración Electrónica de España (PAe) [12] y se encuentra estructurada en tres libros.

- MAGERIT v3 Libro I - Método: describe los fundamentos teóricos de la metodología y ofrece guías para la elaboración de análisis de riesgos, procesos de gestión de riesgos, proyectos de análisis de riesgos, planes de seguridad y consejos prácticos.
- MAGERIT v3 Libro II - Catálogo de Elementos: describe la clasificación de los activos según su tipo y dimensiones de valoración. Además, nos ofrece un catálogo de amenazas y salvaguardas que podremos emplear para disminuir el riesgo.
- MAGERIT v3 Libro III - Guía de Técnicas: describe algunas técnicas generales y especificas utilizadas en análisis y gestión de riesgos.

4.4.1. Método de análisis de riesgos Magerit v3.

El método de análisis de riesgos propuesto por Magerit v3 en el libro I – Método, que emplearemos en el TFM, está formado por una serie de tareas y actividades que describen con

exactitud el proceso que debe de realizar, de acuerdo a la relación entre los elementos [9] (en la página 22) y que pueden verse en la figura 3.

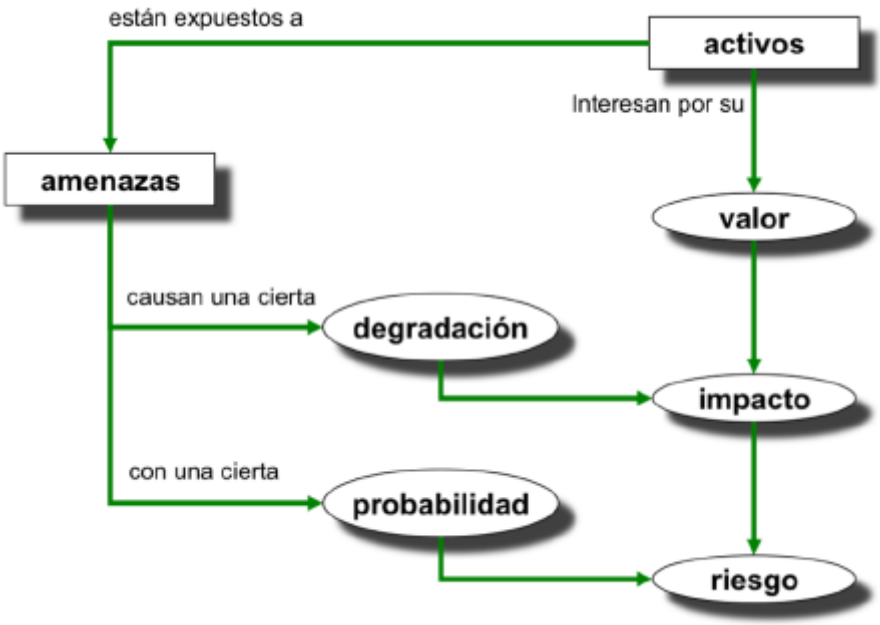


Figura 3. Análisis de riesgos potenciales. (Fuente MAGERIT v3 Libro I)

A continuación, se describen brevemente los procesos descritos en la metodología.

PASO 1: Identificar los Activos

El primer paso descrito en la metodología MAGERIT v3, es la elaboración de una lista conformada por los elementos a proteger, aquellos que suponen un cierto valor para la organización y son necesarios para el buen hacer de esta.

Según la Norma UNE 71504:2008 un activo es definido como "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos." [9] (en la página 22)

Estos activos son detallados y clasificados según la clasificación establecida en MAGERIT v3 - Libro II - Catálogo de Elementos [10] (en las páginas 7-13):

- **[D] Datos** que materializan la información.
- **[S] Servicios** auxiliares o de soporto que se necesitan para poder organizar el sistema.
- **[SW] Software**. Las aplicaciones informáticas que permiten manejar los datos.

- **[HW] Hardware**. Equipos informáticos que permiten hospedar datos, aplicaciones y servicios.
- **[MEDIA] Soportes de información** que son dispositivos de almacenamiento de datos.
- **[AUX] Equipamiento auxiliar** que complementa el material informático.
- **[COM] Redes de comunicaciones** que permiten intercambiar datos.
- **[L] Instalaciones** que acogen equipos informáticos y de comunicaciones.
- **[P] Personas** que explotan u operan todos los elementos anteriormente citados.

Cada tipo de activo se encuentra en riesgo de sufrir ciertos tipos de amenazas, las cuales puede mitigar empleando ciertas salvaguardas que reduzcan ese riesgo.

Los activos forman entre si dependencias, creando así un árbol de dependencias donde los activos de la cima dependerán de los activos de la base. De esta forma, se puede apreciar de forma sencilla como en el caso de materializarse un daño, este daño se extendería desde los activos inferiores hacia los activos superiores. La estructura de dependencias variar entre diferentes organizaciones, ya que cada una tiene sus propias prioridades y características.

Para determinar el interés de una organización en un activo, se establece una valoración que permite determinar la prioridad en el proceso de protección de los activos, desde el punto de vista del daño que causaría su pérdida o deterioro. El valor de un activo contendrá además la suma de los valores de los activos que dependen de este.

Esta valoración se determina evaluando las dimensiones de seguridad o características que le dan valor a un activo. El primer libro de la metodología MAGERIT v3 define 5 dimensiones de seguridad: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Las dimensiones se emplean para valorar las consecuencias de la materialización de una amenaza y como medida del daño para la organización si el activo se ve dañado en dicha dimensión.

En MAGERIT v3 - Libro II - Catálogo de Elementos [10] (en las páginas 15-16) se proponen las siguientes dimensiones para la valoración de los activos:

Tabla 2. Dimensiones de valoración. (Fuente MAGERIT v3 Libro II)

Dimensión	
[D] Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]

[I] Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[A] Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]
[T] Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

PASO 2: Determinar las Amenazas

En este paso se realizará la identificación y valoración de las amenazas a las que se pueden encontrar expuestas los activos y que pueden como resultado dañarlos en parte o de forma irreversible.

De acuerdo con la definición dada por la Norma UNE 71504:2008 [9] (en la página 27) una amenaza es "Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización."

Las amenazas se pueden clasificar en cuatro tipos de acuerdo al origen de esta, según la clasificación establecida en MAGERIT v3 - Libro II - Catálogo de Elementos [10] (en las páginas 25-47):

- **[N] Desastres Naturales:** como terremotos, inundaciones, incendios, etc. Aquí el sistema es víctima pasiva pero debemos contemplarlos.
- **[I] De origen Industrial:** desastres que se dan por las mismas condiciones de la industria donde se desarrolla la actividad (fallo eléctrico, contaminación...).
- **[E] Errores y fallos no intencionados:** ya sean causados por errores hardware, software o problemas causados por personas sin malas intenciones.
- **[A] Ataques intencionados:** ataques deliberados con ánimo de beneficiarse indebidamente o causar daños y perjuicios a los propietarios.

Cada amenaza solamente afectara a ciertos tipos de activos y solo en determinadas dimensiones de ese activo, por lo que es necesario tener constancia de a qué tipo de activos y en que dimensiones puede afectar una amenaza. Por ejemplo, un corte prolongado de la red hacia el exterior de la organización afectará a los activos que necesiten de la red, pero no a la maquinaria industrial que continuará realizando sus fabricaciones.

Además, las amenazas no siempre afectarán en un 100% o en 0% a los activos, si no que contaremos con un porcentaje de degradación del sistema y un porcentaje de probabilidad de que la amenaza suceda.

Por ejemplo en un sistema equipado con un Sistema Alimentación Ininterrumpida (SAI), los cortes de luz afectarán al sistema dependiendo del tiempo total del corte del suministro eléctrico, por lo que el funcionamiento del sistema dependerá de la probabilidad de que sea un corte de luz mayor a la capacidad de alimentación del SAI y el daño causado dependerá de los datos o servicios que se pierdan durante ese periodo de tiempo que el sistema este apagado.

El paso 2 se divide a su vez en varias actividades.

ACTIVIDAD 2.1: Determinar el impacto potencial

Para calcular el impacto potencial que una amenaza puede provocar sobre un activo, consideramos el daño que causa la materialización de una amenaza sobre un activo y sobre sus dimensiones [9] (en las páginas 28-29). Este cálculo de impacto potencial se puede realizar de dos formas:

Valor neto, es cálculo del impacto directo que la amenaza tiene sobre el activo.

Valor acumulado, es el cálculo del impacto que se calcula a partir del partir del valor neto más el valor neto de todos los activos que dependen de él.

ACTIVIDAD 2.2: Determinar el riesgo potencial

Se denomina riesgo potencial a la medida de la probabilidad de un daño provocado por una amenaza ocurra sobre un activo. [9] (en las páginas 29-30) El riesgo es un factor que crece junto a junto a la probabilidad de suceso de la amenaza y al impacto, es decir, para que una amenaza suponga un peligro real es necesario que provoque un alto impacto además de contar con una probabilidad de ocurrencia alta. En caso contrario, será una amenaza de bajo riesgo, ya que puede no ocurrir nunca o tener un impacto apenas apreciable.

Al igual que en el cálculo del impacto potencial, el riesgo puede ser neto o acumulado, dependiendo du si el cálculo tiene en cuenta las dependencias de los activos o no.

PASO 3: Salvaguardas

Los pasos anteriores se desarrollan sin tener en consideración las posibles protecciones y salvaguardas existentes en la organización, por lo tanto, los impactos y riesgos calculados son aquellos a los que los activos estarían expuestos en el caso de no existiese ningún tipo de protección. Por ello, en este paso fortaleceremos los activos añadiendo salvaguardas con el objetivo de reducir en todo lo posible el impacto y el riesgo ante las posibles amenazas que tengan mayor probabilidad de afectar al activo. El coste de aplicar salvaguardas puede ser bastante elevado, por lo que tendremos que centrarnos en aplicarlas sobre los activos esenciales y en las amenazas con mayor riesgo. Para ello, es necesario evaluar bien que salvaguarda emplear para cada amenaza teniendo en cuenta las dimensiones del activo, ya que cada salvaguarda tiene una finalidad y solo afectará a determinadas dimensiones en su protección.

El uso principal de las salvaguardas es el de: limitar la degradación y el de reducir la probabilidad de amenaza [9] (en las páginas 31-32). La figura 4 ilustra como las salvaguardas influyen sobre la probabilidad de que una amenaza se materialice y degradación que esta podrá causar, produciendo una reducción en el impacto y riesgo. Ambos, se consideraran residuales a partir del establecimiento de las salvaguardas.

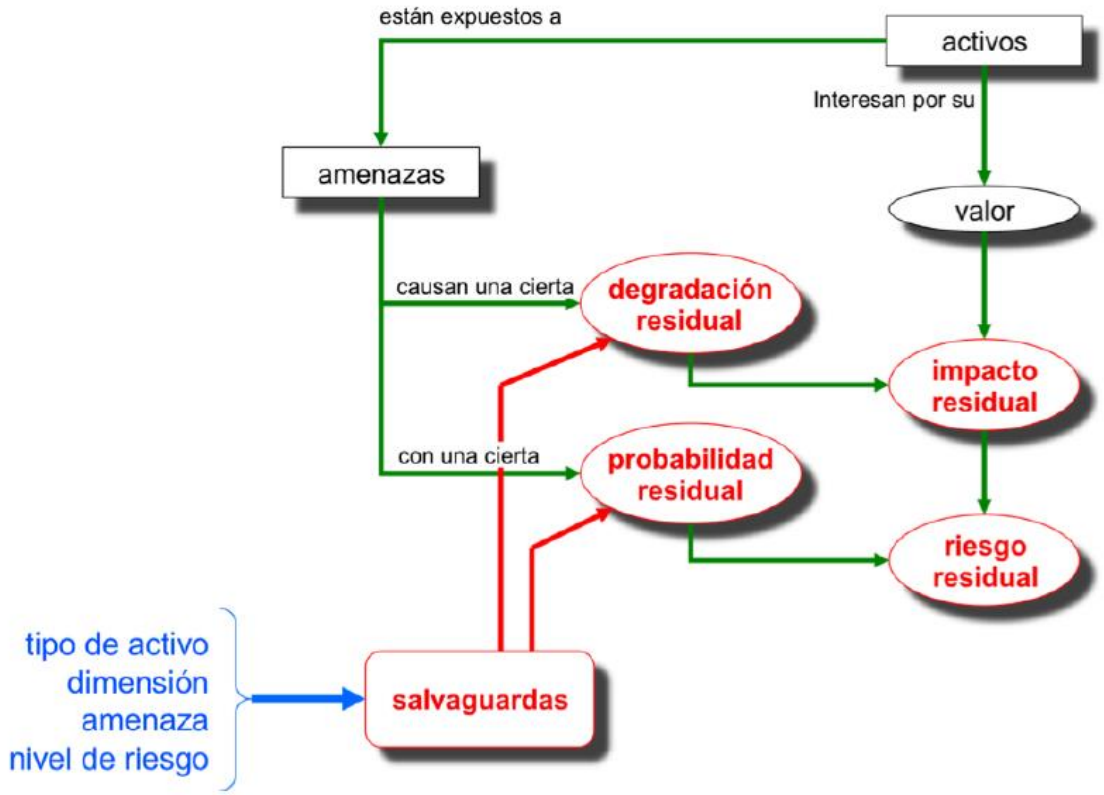


Figura 4. Análisis del riesgo residual con salvaguarda aplicada (Fuente MAGERIT v3 Libro I)

Con el objetivo de limitar la degradación y el de reducir la probabilidad de amenaza, las salvaguardas se pueden catalogar en los siguientes tipos:

- [PR] Prevención: reducen la probabilidad de que una amenaza se materialice.
- [DR] Disuasión: reduce las probabilidades de que un atacante se atreva a materializar una amenaza o se lo piensen antes de intentarlo.
- [EL] Eliminación: se reduce a cero la posibilidad de materialización de una amenaza.
- [IM] Minimización del impacto: acota el impacto de una amenaza.
- [CR] Corrección: medidas para reparar el sistema tras la materialización de una amenaza.
- [RC] Recuperación: medidas para volver al estado anterior de la materialización de la amenaza.
- [MN] Monitorización: medidas que permiten la comprobación paso a paso de lo que está ocurriendo o ha ocurrido.
- [DC] Detección: detección inmediata de la materialización de una amenaza.
- [AW] Concienciación: formación del personal que tiene influencia sobre el sistema.
- [AD] Administración: salvaguardas relacionadas con componentes de seguridad del sistema.

Cada tipo de salvaguarda se relaciona con los objetivos de limitar la degradación y el de reducir la probabilidad de amenaza, de la siguiente forma:

Tabla 3. Tipos de salvaguardas según el modelo de reducción de la degradación y la probabilidad

Efecto	Tipo
Prevenir: reducen la probabilidad	[PR] Preventivas [DR] Disuasión [EL] Eliminación
Limitar: limitar la degradación	[MI] Minimización [CR] Corrección [RC] Recuperación
Fortalecer: reforzar el efecto de las demás	[MN] Monitorización [DC] Detección [AW] Concienciación [AD] Administración

Además, según la clasificación establecida en MAGERIT v3 - Libro II - Catálogo de Elementos [10] (en las páginas 53-57), las salvaguardas se pueden clasificar de forma más particular de acuerdo a su ámbito de aplicación: protecciones generales u horizontales, protección de las claves criptográficas, protección de los servicios, protección del software, protección del hardware, protección de las comunicaciones, protección en los puntos de interconexión con otros sistemas, protección de los soportes de información, protección de los elementos auxiliares, protección de las instalaciones, relativas al personal, de tipo organizativo, de la continuidad de las operaciones, externalización y de adquisición o desarrollo.

En selección de salvaguardas inicial, se realizará un cribado de todas aquellas salvaguardas que: **no sean aplicables**, técnicamente no son apropiadas, no protegen la dimensión necesaria o no protege frente a una amenaza y **no se justifique su uso**, siendo la medida desproporcionada al riesgo. Para este cribado hay que tener en cuenta:

- El tipo de activos a proteger y dimensiones de seguridad a proteger, enfocándonos a los más valiosos.
- Las amenazas que necesitamos evitar o reducir, contemplando las más probables y de mayor impacto.
- Si existen más de una salvaguarda aplicable, consideramos la que mayor cobertura proporciona.

El listado completo de salvaguardas que aplicaremos en este proyecto, se puede encontrar en MAGERIT v3 - Libro II - Catálogo de Elementos [10] (en las páginas 53-57).

El paso 3 se divide a su vez en varias actividades.

ACTIVIDAD 3.1: Determinar el Impacto residual

Tras el despliegue de las salvaguardas con su respectivo proceso de gestión, el nivel de degradación al que se encontraban sometidos los activos, se verá reducido según la eficacia de las salvaguardas [9] (en la página 35). Por lo tanto, será necesario recalcular el impacto que puede tener la misma amenaza sobre el activo teniendo en cuenta la salvaguarda y las dimensiones en las que tiene representación. Esta fase permite valorar el impacto de las salvaguardas sobre los riesgos y será útil a la hora de determinar el valor de la aplicación de salvaguardas.

ACTIVIDAD 3.2: Determinar el riesgo residual

Tras el despliegue de las salvaguardas con su respectivo proceso de gestión. El riesgo al que se encontraban sometidos los activos, se verá reducido según la eficacia de las salvaguardas [9] (en la página 35). Por lo tanto, será necesario recalcular el riesgo que puede tener el impacto de la misma amenaza sobre el activo teniendo en cuenta la salvaguarda y las dimensiones en las que tiene representación.

4.5. Plan Director de Seguridad.

Tal y como se explica en el Libro I – Método de Magerit v3 [9] (en la página 73), el Plan Director de Seguridad (PDS) son el conjunto de proyectos mediante los cuales las decisiones adoptadas para el tratamiento de riesgos se materializan. Una vez conocidas las amenazas que pueden afectar a los activos de la organización, con su análisis de riesgos y salvaguardas, es cuando se puede elaborar el Plan de Seguridad, con el objetivo de programar la aplicación de las salvaguardas de forma planificada.

El plan de seguridad consta de 3 tareas que se deben seguir en orden para elaborar para concluir la elaboración del plan.

4.5.1. Tarea PS.1: Identificación de proyectos de seguridad

En esta tarea el objetivo es elaborar un conjunto armónico de programas de seguridad, lo que es decir, dada una amenaza y un tratamiento de riesgo, indicar las tareas a realizar para implantar sus salvaguardas.

Un proyecto de seguridad estará formado por la agrupación de varias de estas tareas. La agrupación podrá realizarse por conveniencia, bien porque son tareas que de forma aislada no tendrían sentido, bien porque tratan un objetivo común o porque competen a una única unidad de acción. Tal y como se indica en el Libro I de la metodología MAGERIT v3 [9] (en las páginas 73-74), cada programa de seguridad debe describir los siguientes puntos:

- Objetivo genérico.
- Las salvaguardas a implantar o mejorar, detallando el objetivo de la aplicación de la salvaguarda.

- Describir los activos a los que afecta, el tipo de estos, las amenazas afrontadas, la valoración de activos y amenazas y el nivel de impacto y riesgo de estas.
- El responsable de la ejecución del programa.
- Una estimación de costes tanto económicos como de esfuerzo pudiendo valorar:
    - costes de adquisición (de productos), o de contratación (de servicios), o de desarrollo (de soluciones llave en mano), pudiendo ser necesario evaluar diferentes alternativas.
    - costes de implantación inicial y mantenimiento en el tiempo.
    - costes de formación, tanto de los operadores como de los usuarios, según convenga al caso.
    - costes de explotación.
    - impacto en la productividad de la Organización.
- Una relación de subtareas a afrontar, teniendo en cuenta:
    - cambios en la normativa y desarrollo de procedimientos.
    - solución técnica: programas, equipos, comunicaciones e instalaciones.
    - plan de despliegue.
    - plan de formación.
- Una estimación del tiempo de ejecución desde su arranque hasta su puesta en operación.
- Una estimación del estado de riesgo (impacto y riesgo residual a su compleción).
- Un sistema de indicadores de eficacia y eficiencia que permitan conocer en cada momento la calidad del desempeño de la función de seguridad que se desea y su evolución temporal.

En el caso de que el proyecto de seguridad alcance una gran complejidad, estos puntos serán bastante difíciles de concretar, por lo que bastará con proponer unas indicaciones orientativas.

4.5.2. Tarea PS.2: Planificación de los proyectos de seguridad

El objetivo de esta tarea será el de ordenar en el tiempo los proyectos de seguridad. Tal y como se indica en el Libro I de la metodología MAGERIT v3 [9] (en la página 75), los proyectos se ordenarán teniendo en cuenta los siguientes puntos:

- la criticidad, gravedad o conveniencia de los impactos y/o riesgos que se afrontan, teniendo máxima prioridad los programas que afronten situaciones críticas.

- el coste del programa.
- la disponibilidad del personal propio para responsabilizarse de la dirección (y, en su caso, ejecución) de las tareas programadas.
- otros factores como puede ser la elaboración del presupuesto anual de la Organización, las relaciones con otras organizaciones, la evolución del marco legal, reglamentario o contractual, etc.

El plan de Seguridad suele planificarse empleando tres niveles de detalle.

- Plan director (único): establecen las directrices de actuación a largo plazo, en un periodo de 3 a 5 años.
- Plan anual (una serie de planes anuales): trabaja con planes de 1 o 2 años con los programas de seguridad en cada uno de ellos.
- Plan de proyecto (un conjunto de proyectos): típicamente de corta duración (de menos de 1 año) y establece el plan detallado de ejecución de cada programa de seguridad.

Se debe desarrollar un Plan Director único, ya que es el que da perspectiva y unidad de objetivos a las actuaciones puntuales. A partir del Plan Director, ya se permite ir desarrollando planes anuales que, dentro del marco estratégico, van estructurando la asignación de recursos para la ejecución de las tareas, en particular partidas presupuestarias. Y por último, el plan de trabajo de cada proyecto.

4.5.3. Tarea PS.3: Ejecución del Plan

Finalmente y tras el resto de tareas, se realiza la ejecución del Plan Director siguiendo las directrices marcadas en los planes anuales y de proyecto, para así lograr la implantación exitosa de las salvaguardas, la generación de normativas, la formación del personal y el resto de resultados que permitirán obtener un nuevo estado de riesgo aceptable por parte de la organización [9] (en la página 76).

4.6. Plan de contingencia y continuidad de negocio.

El desarrollo de Plan Director de Seguridad nos permite prevenir las circunstancias que pueden afectar a nuestra entidad, con el objetivo de evitar todas aquellas amenazas que puedan provocar un riesgo. Pero el riesgo cero no existe, por lo que se debe completar el Plan Directo de Seguridad con otros elementos que nos permitan recuperarnos de un desastre a la vez que nos permitan mantener la continuidad del negocio. Aquí entran en juego los Planes de contingencias y continuidad de negocio.

Una buena planificación de recuperación de la actividad normal por parte de una empresa ante un desastre permitirá minimizar el impacto económico que pueda ocasionar la materialización de la amenaza, evitar la fuga o robo de información crítica, evitar problemas legales y repercutirá favorablemente a la imagen y reputación de la empresa.

Para nuestro plan de contingencia y de continuidad de negocio, vamos a usar como base el Plan de Contingencia y Continuidad de Negocio de la Colección protege tu empresa elaborado por INCIBE (Instituto Nacional de Ciberseguridad de España).

Los objetivos de un plan de contingencia serán los siguientes [13] (en las páginas 3-4):

- Lograr que ante una incidencia se mantenga el nivel de servicio en los límites definidos. La organización debe continuar con su actividad de una forma que los usuarios no se vean lo más mínimamente afectados.
- Establecer un periodo de recuperación acotado. Se debe de considerar cual es el tiempo de recuperación aceptable y marcar mecanismos para lograr, en ese tiempo, volver a tener operativos sistemas que permitan desarrollar la actividad del negocio.
- Recuperar la situación inicial antes del incidente, marcando los pasos, estrategias y procedimientos necesarios para lograr volver al estado antes de que ocurriera el desastre.
- Analizar los resultados y motivos de los incidentes, para así reconsiderar si es necesario en el Plan Director de Seguridad, reestimar amenazas, impactos y riesgos, y las salvaguardas a aplicar.

Para materializar un plan de contingencias, se deben desarrollar las siguientes fases [13] (en las páginas 7-8) que nos permitirán analizar desde un punto formal aquellos factores que garantizan la continuidad de la empresa, permitiendo que la actividad de la empresa no se vea resentida.

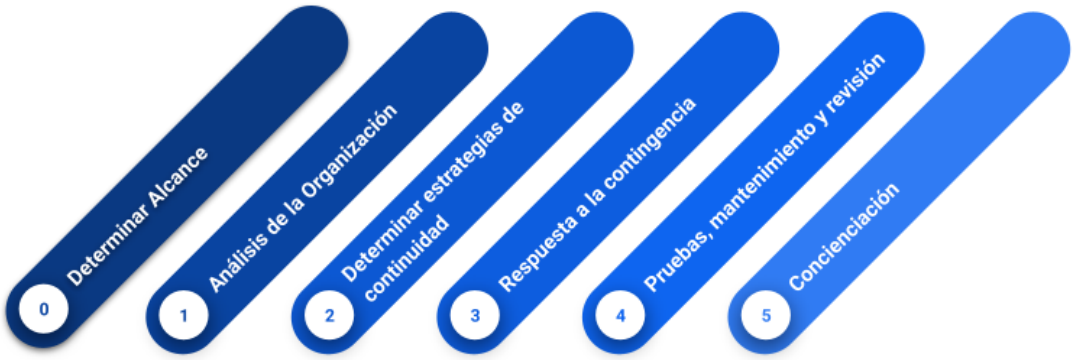


Figura 5. Fases de un Plan de Contingencias (Elaboración propia)

FASE 0: Determinar alcance

En esta fase se determinarán los elementos de la organización que serán el foco del plan de continuidad. A la hora de decidir un elemento, se comienza por los sistemas o procesos de mayor criticidad, pudiendo realizar un enfoque por activo o por proceso (como por ejemplo, la producción). Ya que el objetivo principal es la continuidad del negocio, se recomienda emplear un enfoque por procesos a partir del cual se detallen las acciones sobre los activos que forman parte del proceso.

FASE 1: Análisis de la organización

En esta fase paso se realizará la obtención, elaboración y comprensión de las circunstancias, tecnologías, procesos y recursos de la organización, orientadas a los procesos críticos.

Durante esta fase se realizarán reuniones con el personal con el objetivo de obtener las dependencias de proveedores, personal implicado, aplicaciones, recursos y datos que se necesitan.

También se realizará un análisis formal del impacto sobre el Negocio o BIA (Business Impact Analysis) con el que obtendremos los requisitos temporales y de recursos necesarios para definir los procesos de continuidad y también influirá sobre aspectos de los planes de seguridad.

En el caso de que no dispongamos del análisis de riesgos, será muy importante elaborarlo, ya que necesitaremos conocer que amenazas se ciernen sobre nuestros servicios. Este análisis de riesgos nos aporta en detalle los activos de información y su relevancia para la empresa, las amenazas a las que están sujetos, el impacto de estas y su probabilidad de ocurrencia junto a la degradación que producen, y el tratamiento que se realiza en cada una para minimizar sus posibles efectos de forma preventiva.

FASE 2: Determinar la estrategia de continuidad

En esta fase debemos determinar las estrategias para recuperar el sistema de forma que se asegure no exceder el MTD del proceso. Para ello, es necesario asegurar que los RTO implicados no exceden dicho MTD, logrando así que una contingencia no degrade el sistema hasta tal punto de ser irreversible el daño.

La estrategia debe considerar todas las acciones a realizar desde el momento en el que se detecta el problema hasta que se logra volver a un estado óptimo.

FASE 3: Respuesta a la contingencia

En esta fase se implementarán las estrategias diseñadas en las fases anteriores. Dispondremos de un plan de acción ante una incidencia, desde el momento de la crisis, hasta la puesta en marcha y recuperación del sistema. Para ello, analizamos, agrupamos y priorizamos las medidas establecidas en la estrategia de continuidad, para establecer los siguientes planes:

- Plan de crisis. Este documento tiene como objetivo gestionar los momentos iniciales de la crisis, con los siguientes puntos bien definidos: condiciones de disparo, flujos de toma de decisiones, medios para declarar una situación de crisis, personal responsable de la situación de crisis, datos de contacto de los responsables, niveles de priorización de recuperación de la infraestructura, requisitos temporales de puesta en marcha y los planes operativos y personal responsable.
- Plan operativo de recuperación de entorno. Es el plan de recuperación de cada uno de los entornos que han sido afectados por la incidencia, tomando como referencia los procedimientos técnicos de trabajo determinados en la estrategia de continuidad.
- Procedimientos técnicos de trabajo. Es la documentación que describe como realizar las tareas técnicas para la gestión y recuperación de una aplicación, sistema, infraestructura o entorno. Se elabora como una lista de instrucciones que se deben ejecutar en orden.

FASE 4: Pruebas, mantenimiento y revisión

Con el afán de que los procedimientos anteriormente explicados se encuentren actualizados y funcionales ante cualquier tipo de cambio, será necesario realizar un plan de pruebas y mantenimiento.

Plan de mantenimiento. Este plan se encarga de mantener actualizada toda la documentación cada vez que se produzca un cambio sobre un elemento del sistema, de forma que la información de los planes siempre se encuentre actualizada.

Plan de pruebas. En este plan se detallan aquellas pruebas que deben ser llevadas para asegurar que los planes se encuentran actualizados y para comprobar la capacidad que la organización sería capaz de enfrentarse ante una crisis y lograr recuperarse de un desastre.

FASE 5: Concienciación

En este paso se realizarán una serie de tareas que ayudaran a concienciar al personal de la organización de la importancia de los planes de continuidad. Para ello, contaremos con dos tipos de formaciones para el personal:

- Formación general. Consiste en hacer a todo el personal de la empresa participe del sostenimiento de la ciberseguridad, mediante el desarrollo de campañas informativas, actividades, pequeños talleres y charlas, de forma complementaria a la actividad de la empresa.
- Formación específica. Consiste en la formación únicamente de los responsables y expertos técnicos de la organización con el objetivo de ser capaces de manejar todas las herramientas necesarias para proteger a la empresa y hacerlo con la máxima efectividad y eficiencia.

Para el diseño de la campaña de concienciación, una buena estrategia es el desarrollo de acciones de concienciación para empleados. Acciones dirigidas con el objetivo que eliminar una mala práctica extendida en la empresa, evitar un tipo de cibercrimen que este en apogeo o formar sobre alguna nueva medida implantada que sea necesaria adoptar por todo el personal.

4.7. Antecedentes.

Durante mis años de experiencia laboral, tuve la oportunidad de trabajar en el área de IT para un grupo empresarial que había crecido muy rápidamente en los años anteriores a mi incorporación, por lo que pude comprobar de primera mano la necesidad de adaptar las infraestructuras informáticas a la creciente demanda de servicios que el grupo empresarial requería para poder adaptarse a las nuevas normativas y volúmenes de pedidos a los que debían de enfrentarse.

Este grupo empresarial, amplió en un corto espacio de tiempo varias veces sus instalaciones, pasando de ser una sola empresa a un grupo formado por varias empresas bajo la misma dirección administrativa y bajo la responsabilidad del mismo departamento de informática. Por

lo tanto, tuvimos que interconectar progresivamente los sistemas de cada una de las empresas bajo la misma estructura informática y las mismas herramientas de administración y gestión.

La organización cuenta con ciertos procedimientos que diseñamos y registramos en una wiki destinada como información de soporte para el departamento de informática. En estos procedimientos explicamos, paso a paso, las acciones que hay que realizar para recobrar la estabilidad del sistema a la hora de: realizar y restaurar copias de seguridad, detectar e impedir intentos de acceso no autorizados, caída y recuperación de la red, ver los sistemas comprometidos por el acceso de un programa malicioso por el correo corporativo.

Todos estos procedimientos vinieron previamente de sufrir estos tipos de problemas en los sistemas de la organización, para en el caso de que volviese a ocurrir poder reaccionar de una forma más inmediata a la solución del problema. A pesar de contar con ciertos procedimientos, no hay nada formalizado documentalmente, por lo que no se cuenta con ningún plan a nivel organizativo.

Con el Plan Director de Seguridad, los planes de contingencia y concienciación, se pretende formalizar todos estos procedimientos en Planes de Seguridad a disposición de la organización, además de obtener la involucración y concienciación, de la dirección y el personal, en la protección de los sistemas de la información.

5. Objetivos

El objetivo de este proyecto es el diseño e implantación de un Sistema de Gestión de la Seguridad de la Información en un grupo empresarial, que permita asegurar la integridad, la autenticidad, la confidencialidad y la disponibilidad de la información.

El grupo empresarial contempla la posibilidad de llegar a generar una certificación a partir de la implantación del SGSI, pero en este trabajo nos centraremos exclusivamente en los procedimientos para implantar un SGSI.

Al tratarse de un grupo empresarial con una gran cantidad de activos y ya que el objetivo del TFM es abordar todas las acciones necesarias, desde el análisis hasta el desarrollo de planes de contingencias y continuidad, si fuese necesario se priorizarán las actuaciones seleccionando solo el catálogo de activos de mayor valor sobre los que generar el plan, estableciendo así los procedimientos, bases y plantillas para el trabajo con el resto de activo que queden sin tratar. El objetivo principal del trabajo es establecer los procedimientos y herramientas formales del SGSI, y en la medida que den tiempo implementarlos para todos los activos. A partir de esta selección, desarrollare una propuesta de Plan Director de Seguridad, planes de continuidad y planes de concienciación con la finalidad de que la dirección de la empresa los evalué, apruebe e implante, si consideran que es rentable asumir el coste ante el beneficio que los planes aportarán.

Para completarlo, marcaremos los siguientes objetivos:

1. Estudio del grupo empresarial. Análisis de su contexto, modelo de negocio, estructura organizativa, la infraestructura tecnológica y la información con la que la empresa cuenta para el buen desarrollo de su labor.
2. Elaboración del catálogo de activos y selección. Definir un listado con los elementos de la infraestructura tecnológica y su valoración en función de la importancia para el funcionamiento de la empresa. Realizar un estudio de aquellos que deben ser protegidos con mayor premura.
3. Emplear la metodología MAGERIT para desarrollar los Planes de Seguridad. Teniendo en cuenta los activos seleccionados: elaborar el listado de amenazas, realizar el análisis de riesgos, realizar el análisis de salvaguardas y diseñar los planes de seguridad.

4. Desarrollar planes de contingencia y continuidad de negocio. A partir de las amenazas determinadas, definir los planes de continuidad de negocio, incluyendo un plan de formación y concienciación en materia de ciberseguridad como parte del Plan Director de Seguridad.
5. Implantación. Proporcionar a la empresa el Plan Director de Seguridad desarrollado para su evaluación e implantación progresiva de las medidas propuestas en el plan.

6. Estudio del contexto del grupo empresarial

En este capítulo, realizaremos el estudio del contexto del grupo empresarial donde incluiremos una presentación de la organización y especificaremos su estructura, aspectos técnicos, políticas de seguridad, además de la realización de un análisis del estado actual del SGSI.

6.1. Introducción

El grupo empresarial Anónima S.L., dedicado a la creación y diseño de muebles a medida, fue fundado a finales de la década de los 90 por parte de los actuales gerentes. Actualmente, trabajan mayoritariamente para grandes cadenas de supermercados por todo el territorio español y algunas en el extranjero.

Originalmente, se trataba de una pequeña empresa localizada en una localidad de la provincia de Alicante, donde a día de hoy se sigue localizando la sede del grupo, con su fábrica y oficinas. Recientemente, por la necesidad de implantar nuevos servicios, se han visto obligados a crecer muy rápidamente, creando varias empresas menores dedicadas a la fabricación de diferentes tipos de productos, hasta acabar construyendo el grupo empresarial Anónima S.L.

Dentro de la actividad de negocio, se podría distinguir entre dos líneas: el diseño y montaje de muebles; y otra línea relacionada con trabajos de fabricación de piezas de metal, plástico, acrílico y madera. Antiguamente, la fabricación de estas piezas era subcontratada; pero con el crecimiento del grupo, ahora forma parte de la propia línea de negocio de la empresa, produciendo gran cantidad de piezas para otras empresas de la provincia como ACTIU S.L., dedicada a la fabricación de mobiliario de oficina.

Figura 6. Proceso de negocio de Anónima S.L. (Fuente propia)

A día de hoy, el grupo empresarial, cuenta con varias naves industriales repartidas dentro de la misma localidad. En cada una de estas naves industriales, se realizan unos procesos industriales diferentes, separando así los trabajos de diseño y prototipo, de los de fabricación, pintura, montaje… Todas ellas, se encuentran interconectadas a través de teléfono e Internet.

El grupo empresarial cuenta además con varias empresas proveedoras de suministros y subcontratadas, que les permiten agilizar el trabajo y los transportes. La relación con estas empresas se realiza por los métodos tradicionales de contacto, correos electrónicos y llamadas telefónicas.

El grupo cuenta con un portal web, destinado a la red de clientes finales para que puedan conocer los servicios que presta la empresa y consultar las últimas novedades, anuncios y ofertas. Para ayudar a las ventas, el grupo empresarial cuenta con una red de comerciales por todo el territorio nacional y algunos en el extranjero.

Internamente, el grupo empresarial cuenta con un Sistema de Planificación de Recursos Empresariales o ERP (“Enterprise Resource Planning”), el cual da soporte a la gestión de la actividad empresarial. Este ERP en sus comienzos fue configurado inicialmente con ayuda de una empresa externa, pero actualmente el departamento de informática cuenta con la formación suficiente para realizar nuevas configuraciones sobre el ERP a medida de la empresa. Además, cuenta con varios programas de gestión de la producción hechos a medida, a través del cuales se va controlando la producción y las incidencias que puedan surgir.

Por parte de los usuarios clientes, esperan de Anónima S.L. que los servicios prestados se adecuen a las condiciones contractuales, por lo que la empresa debe garantizar siempre la disponibilidad de los servicios a través de los cuales se gestionan las incidencias, al igual que proteger adecuadamente la información, ya que en caso contrario serían las empresas asociadas las que recibirían las quejas de los clientes y sus posibles reclamaciones.

6.2. Estructura

La empresa se organiza con una estructura en la que Anónima S.L. actúa como matriz de un grupo de empresas las cuales van siendo creadas para la gestión de las diferentes producciones que se requieran, mientras Anónima, S.L. se encarga del resto de actividades y gestión

A su vez, se organiza mediante los siguientes departamentos, tal y como se puede ver en la siguiente figura realizada a partir del organigrama de la empresa.

Figura 7. Estructura organizativa de Anónima S.L. (Fuente propia)

Dirección o Gerencia: este departamento, está formado por los dos directores de la empresa. Uno de ellos se dedica a supervisar al resto de departamentos de producción y diseño, mientras que el otro, supervisa a los departamentos comerciales y financieros.

Responsable del Sistema de Gestión Integrado: es el responsable en establecer los protocolos de actuación a seguir en el día a día de la actividad productiva a nivel empresarial. Se encarga de procurar que la empresa siga las normas ISO y de ayudar a la implantación de las nuevas normas que la empresa necesite para cumplir con nuevas certificaciones.

Departamento comercial: es el departamento responsable de captar nuevos clientes y de su fidelización. Los comerciales se reúnen con los directivos de las empresas clientes para ofrecer sus servicios y establecer lazos de confianza entre empresas. Cada cierto tiempo, se generan recursos informativos hacia los clientes, para mostrar nuevos servicios y aumentar la confianza en la empresa.

Departamento financiero: es el departamento responsable de gestionar toda la información contable de la empresa para el cumplimiento de las obligaciones fiscales, para esa labor utiliza software especializado en gestión de facturación y contabilidad.

Recursos humanos: departamento responsable de la gestión del personal de la empresa. Se encarga de realizar los procesos de selección de personal, del pago de las nóminas, de la búsqueda de la formación para el nuevo empleado y de la formación de contratos con el personal de la empresa.

Departamento de compras: este departamento está dedicado a la solicitud de materias primas y establecer contactos con las empresas subcontratadas para pedirles aquellos servicios requeridos por la empresa en un determinado momento.

Departamento de ventas: este departamento está dedicado a gestionar la venta de productos terminados y semielaborados a otras empresas que las soliciten, a realizar la logística y contratar el envío de los pedidos para cumplir con los plazos acordados con el cliente.

Departamento de diseño: en este departamento se realiza el diseño de los muebles a gusto del cliente, comenzando desde los prototipos hasta los diseños finales. Para ello, se usan herramientas de dibujo por ordenador y software de diseño 3D por ordenador.

Departamento técnico: este departamento, toma los diseños del departamento de diseño, y realizan el despiece para elaborar el mapa de fabricación del producto. También producen los mecanizados que son leídos por las máquinas para cortar las piezas. Además, envían solitudes de materias primas a comprar al departamento de compras Usan herramientas de diseño 3D muy especializados.

Departamento de producción: este departamento, se encarga de crear los grupos de trabajo y supervisar el trabajo de los operarios, controlando los procesos para tratar de llevar la fabricación en los tiempos establecidos. Usan un software para el control de la producción.

Departamento informático: se dedica a la instalación y mantenimiento de todos los ordenadores de la empresa, de la compraventa de material informático y del control de las

redes. Además, se encargan, del diseño y programación de nuevas herramientas software que son de utilidad a la empresa.

6.3. Aspectos técnicos

Los aspectos técnicos describen los elementos de TI (Tecnologías de la información) con los que cuenta el grupo empresarial. La empresa cuenta con una sede central donde se encuentran sus oficinas en las cuales se encuentran todos los departamentos: producción, financiero, comerciales, técnicos, RR.HH, informáticos…

Estas oficinas cuentan con una red LAN dividida lógicamente a nivel de IP en dos LANs, una para la red de invitados y otra para la red interna propiamente de la empresa, para todos los departamentos y máquinas que requieran conexión a red. La red de invitados es la que se usa también para ofrecer red inalámbrica a los dispositivos móviles que no requieren entrar en la red empresarial.

Para la conexión entre las diferentes naves industriales, se emplea un enlace punto a punto de fibra óptica (fibra oscura) ofrecida por el proveedor local de red y donde no es posible realizar el enlace de fibra oscura, se emplean antenas Mikrotik bidireccionales a 60GHz.

Los equipos informáticos son básicamente de cinco tipos según sus características y propósito: Servidores, equipos de oficina, equipos de diseño, equipos de producción, tabletas de producción y portátiles para comerciales.

Los servidores, los cuales se encuentran en la sede principal de la empresa, son servidores PowerEdge de Dell, con hardware específico de servidor diseñado para estar en funcionamiento 24x7 y tolerancia a errores. En total, se disponen de 4 servidores: uno de virtualización, dos NAS y uno dedicado a las copias de seguridad. El servidor principal de virtualización cuenta con algunos componentes redundados (discos en RAID0 para el sistema, RAID5 Hot Spare para los datos, doble tarjeta de red y doble fuente de alimentación). Mantiene todo el software de red, antivirus, dominio Windows y Active Directory. Se encarga de controlar el acceso de usuarios a la LAN y aplicar las políticas de seguridad sobre los diferentes recursos compartidos de la red. Estos, se encuentran en una habitación cerrada con llave, bajo la responsabilidad del departamento de informática.

Los equipos de oficina son estaciones de trabajo Dell con una configuración de hardware preparada para funcionar correctamente con el software de la empresa, diseñados con

componentes optimizados para uso profesional. La línea base se compone de un monitor de 24" full HD, 8GB RAM, procesador x64 i7, SO Windows 10 Pro, tarjeta red integrada, tarjeta gráfica dedicada, disco SSD 256GB.

Los equipos de diseño son estaciones de trabajo Dell Precision T3610 mucho más potentes que los equipos de oficina. Presentan una configuración de hardware optimizada para funcionar perfectamente con software de diseño y renderizado. Estos equipos cuentan con un monitor de 32" full HD, 24GB RAM, procesador Intel Xeon E5-1600 v2 (con 6 núcleos), SO Windows 10 Pro SP1, tarjeta red integrada, tarjeta gráfica NVIDIA Quadro, disco SSD 512GB. Son utilizados en el departamento de diseño.

Los equipos de producción son ordenadores clónicos, equipados con Windows 10, con una configuración hardware bastante básica para permitir funcionar los programas que se requieren para la producción. Son empleados por los operarios para cargar mecanizados en las máquinas de la producción.

Las tabletas de producción son Samsung Galaxy Tab A6 preparadas con sistemas de protección para ser empleadas en las plantas de producción: protección ante golpes, suciedad, polvo… Se encuentran configuradas únicamente para ofrecer conexión a servicios y aplicaciones de la red interna. Son empleadas por los operarios para fichar tiempos de producción y visualizar planos.

Los ordenadores portátiles, son Dell Latitude E7440 equipados con Windows 10. Estos equipos están diseñados especialmente para viajar con ellos, por lo que presentan bastante resistencia a golpes y un peso muy ligero. Son empleados especialmente por los empleados del departamento comerciales. Para trabajar, se conectan mediante VPN a la red interna de la empresa a través de tarjetas de telefonía móvil o conexiones de datos privadas. El departamento de informática suele recomendar a sus empleados evitar la conexión a la VPN a través de redes públicas, aunque esta recomendación no se encuentra formalizada.

Además de los ordenadores de trabajo de las oficinas, también hay que tener en cuenta que muchas de las máquinas de trabajo como láseres o robots disponen de terminales con Windows XP y Windows 7 embebido. Estos terminales están integrados con las máquinas de producción, el personal de la empresa no tiene acceso a ellas, pero sí que necesitan conexión a la a la red interna de la empresa.

Las herramientas que utilizan son variadas pero la mayoría son aplicaciones de escritorio, como el paquete ofimático que se emplea para realizar documentos, fichas de cálculo y documentos específicos, el paquete de diseño con sus herramientas de diseño en 3D, el paquete de

contabilidad y el ERP de la empresa al que se conectan casi todos los departamentos para realizar sus trabajos.

La página web para clientes se ha desarrollado por una empresa externa y está alojada en un servidor y dominio propios de la empresa externa, sin ninguna relación a la infraestructura propietaria de la empresa.

La administración de los equipos y la administración de los usuarios son realizadas por el departamento de informático, bajo las órdenes de la administración. La política de usuario/contraseña es básica, se establece una contraseña única por departamento que se actualiza una vez al año. Los usuarios son dados de alta por el servicio de informática en un dominio que tienen en uno de los servidores Windows.

El sistema de correo electrónico esta subcontratado a una empresa externa, que ofrece el hosting y las cuentas de usuario. Así pues, no es necesario conectarse a la red de la empresa para poder consultar el correo.

Para el traspaso de documentos internamente, la empresa usa el correo electrónico para aquellos archivos que ocupen menos de 20 megas. También se usa un sistema de carpetas compartidas en uno de los servidores de almacenamiento. El acceso a las carpetas compartidas se puede restringir por usuario o grupo de usuarios del dominio.

La empresa apenas cuenta con documentación. Cuenta con una wiki donde los trabajadores pueden ir creando páginas y editarlas, pero los trabajadores no están muy concienciados de ella, por lo que se encuentra prácticamente en desuso.

6.4. Política de Seguridad de la Información

El grupo empresarial no cuenta con una política de seguridad de la información. La documentación de la que dispone son instrucciones de tipo técnico de algunos procesos documentados por el Departamento de Informática en una wiki interna.

Se ha preparado la empresa para cumplir con la Ley de Protección de Datos [3], por lo que se dispone de cierta documentación al respecto.

No se ha realizado ninguna clase de formación en materia de seguridad de la información a los empleados de la empresa.

El acceso a Internet solamente se encuentra restringido en los equipos destinados a la producción (equipos de producción, terminales de las máquinas y tablets de operación).

No existe una directriz formalizada en cuanto al uso de internet o correo.

No existe una política respecto a la seguridad de las contraseñas, ya que actualmente las contraseñas se encuentran administradas por el departamento de informática.

Los usuarios deben ser dados de alta en el sistema por el departamento de informática para tener acceso a los recursos y sistemas de los que la empresa dispone. Al personal de oficina, se le proporciona una cuenta de correo electrónico destinada al uso profesional.

Existen grupos de seguridad, en los que los usuarios son dispuestos según las necesidades de cada grupo (normalmente, se corresponden a las necesidades de los diferentes departamentos): administración, gerencia, técnicos, contabilidad. Estos grupos se seguridad se aplican tanto al acceso a los recursos de la red corporativa, como al software ERP y de gestión.

6.5. Estado actual SGSI

Para comprobar el estado inicial del SGSI en el grupo empresarial se ha empleado una herramienta del INCIBE [14] que consiste en un documento en Microsoft Excel. Este documento contiene una serie de preguntas de forma categorizada que nos permiten evaluar la seguridad informática dentro de la organización, apoyándonos en los análisis sugeridos por la norma ISO/IEC 27001:2018 [7].

El documento cuenta con secciones a cumplimentar: Los requisitos obligatorios del SGSI y "Estado y Aplicabilidad de controles de Seguridad de la Información" que se basa en el Anexo A de las normas ISO 27001.

Para evaluar el estado actual de los controles, se emplearan 8 estados posibles dependiendo de la gravedad del estado actual del control:

- **Desconocido:** No ha sido verificado.
- **Inexistente:** No se lleva a cabo el control de seguridad en los sistemas de información.
- **Inicial:** Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su existo depende de la buena suerte y de tener personal de alta calidad.
- **Repetible:** La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.

- **Definido:** El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.
- **Administrado:** El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
- **Optimizado:** El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.
- **No aplicable:** A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.

Ya que el documento consta de muchas cuestiones y lo importante para el análisis son las conclusiones que se extraen de ello, este documento con todas las preguntas respondidas ha sido incluido en el ANEXO 1 de este TFM donde puede ser consultado.

Al finalizar los cuestionarios, la herramienta nos devolverá unas graficas que nos mostrarán el estado de actual de la implementación del SGSI. Para este estudio, el análisis nos ha permitido obtener las gráficas que hacen referencia al "Estado de Implementación SGSI" (Figura 8) y al "Estado y Aplicabilidad de controles de Seguridad de la Información" basado en el Anexo A de las normas ISO 27001 (Figura 9).

El estado de la implementación del SGSI en la organización (Figura 8) es prácticamente inexistente. No se dispone de nada formalizado y las medidas de seguridad implantadas se han realizado de un modo totalmente informal.

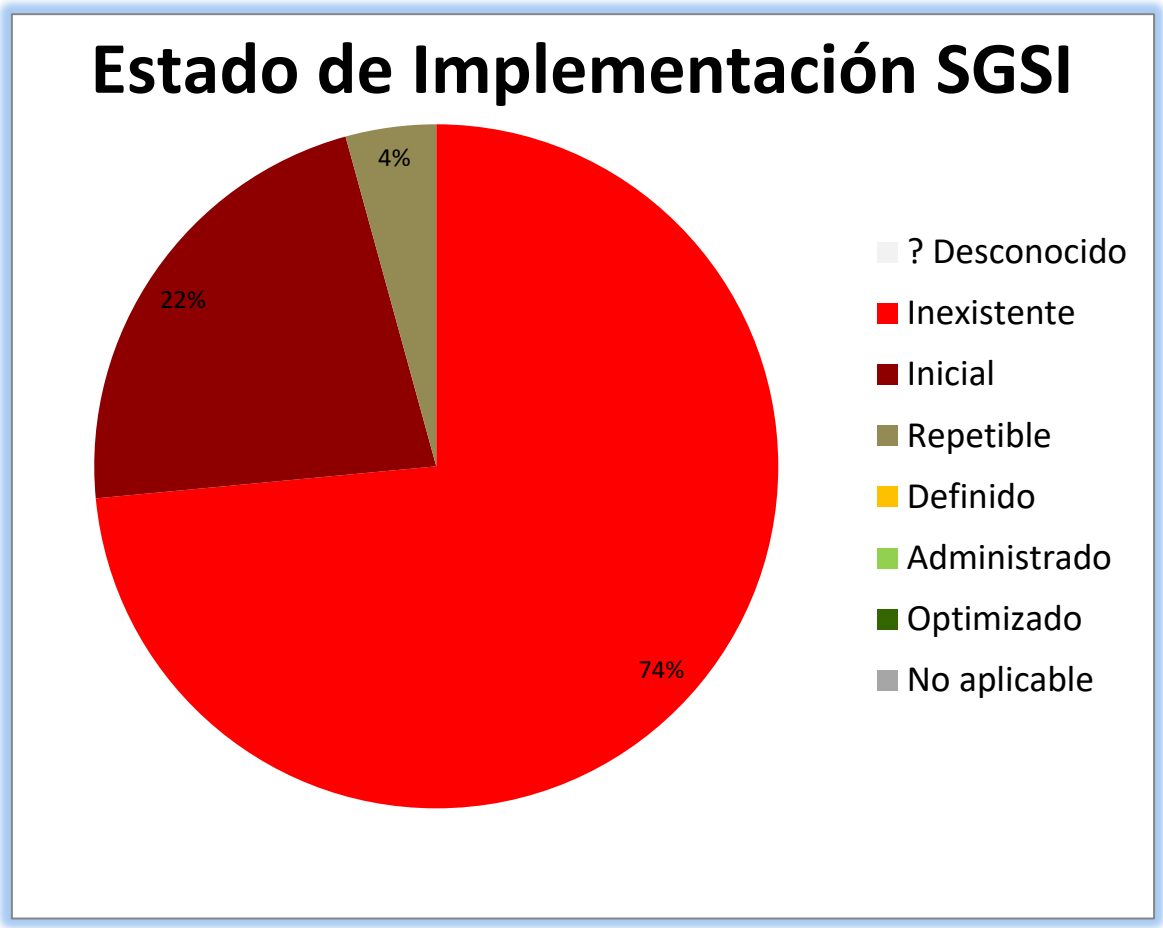


Figura 8. Gráfico del estado de implementación del SGSI en Anónima S.L. (Fuente propia, 2021)

En cuanto al "Estado y aplicabilidad de controles de Seguridad de la Información", el gráfico (Figura 9) muestra la situación inicial de la seguridad informática en el grupo empresarial. A continuación, detallaremos el análisis que hemos obtenido para Anónima S.L.

Figura 9. Gráfico de la situación inicial de la seguridad informática en Anónima S.L. (Fuente propia, 2021)

Observando la gráfica (Figura 9), podemos considerar:

- El grupo empresarial Anónima S.L. tiene 4% de sus procesos de seguridad optimizados, lo que significa que tiene un proceso documentado, aprobado y formalizado, cuya eficacia se mide cada cierto tiempo empleando indicadores. Esto es así, ya que ciertos aspectos de seguridad están asegurados por empresas externas o porque se ha requerido la creación de políticas para cumplir con la legislación y proteger los sistemas.
- El 18% de la seguridad informática se encuentra administrada, lo que significa que se llevan a cabo controles de acuerdo a un procedimiento documentado, aprobado por

dirección y formalizado. Estos controles carecen de controles periódicos, ya sea por falta de personal o de tiempo de los empleados.

- El porcentaje de controles definidos en el grupo empresarial es de un 21%. Estos controles se aplican conforme a un procedimiento documentado, pero no formalizado ni aprobado por la dirección. Estos controles se aplicaron a medida que surgieron nuevas necesidades pero nunca se ha considerado formalizarlas.
- El 14% de la seguridad en el grupo empresarial es repetible. Las medidas de seguridad se realizan de un modo completamente informal, usando procedimientos propios ni documentados.
- Una gran parte de la seguridad del grupo empresarial (el 29%), es inicial. Esto quiere decir, que existen algunas medidas de seguridad, pero no se gestionan ni existe un proceso formal para llevarlas a cabo. El éxito de su eficacia recae bastante en la suerte y en el personal de la empresa. Esta cifra refleja que el grupo empresarial no ha dado demasiada importancia a la seguridad de la información. La concienciación del personal es muy baja en ese aspecto.
- Un 13% de los controles de seguridad establecidos en la ISO27K son inexistentes dentro del grupo empresarial. Esto se debe a la poca madurez de la empresa en materia de ciberseguridad, ya que la criptografía apenas se aplica para la protección de la información en el día a día, la protección por contraseñas es muy básica, el establecimiento de entornos de prueba es nulo y la concienciación del personal es muy pobre en materia de ciberseguridad.
- Un 1% de los controles resultan no aplicables en el contexto del grupo empresarial. Esta cantidad se refleja en que el grupo empresarial no ofrece servicios de internet a sus clientes.

7. Análisis de la seguridad del grupo empresarial

En este capítulo, realizaremos el análisis de la seguridad del grupo empresarial Anónima S.L. Para ello, nos basaremos en el método de análisis de riesgos propuesto en la metodología Mageritt v3 en el libro I – Método, que emplearemos en el TFM. Esta metodología dispone de una serie de tareas y actividades que describen con exactitud el proceso que debe de realizar, para lograr obtener el análisis a partir del cual se puedan establecer los planes de seguridad [9] (en la página 22).

7.1. Inventario de activos

El primer paso que se establece en la metodología de Magerit v3 es el de la elaboración del catálogo de activos de la empresa. Esta tarea consiste en definir un listado con los elementos de la infraestructura tecnológica a proteger y su valoración en función de la importancia para el funcionamiento de la empresa.

En el capítulo 4.4.1. Método de análisis de riesgos Magerit v3, se explica el uso de la metodología Magerit v3 para realizar el inventario, su categorización y la obtención de su valor mediante la evaluación de sus dimensiones de seguridad. Por lo tanto, en este capítulo nos centraremos en definir las escalas de valoración y presentar el inventario de activos obtenido del grupo empresarial.

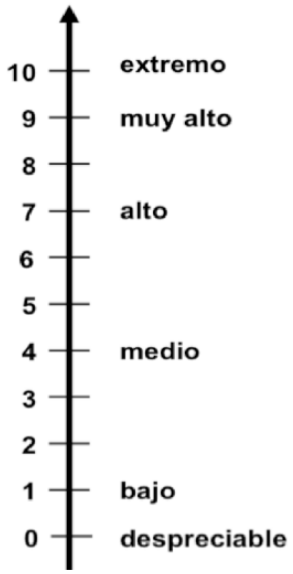
7.1.1. Escalas de valoración

Para realizar una valoración homogénea necesitaremos establecer una escala de valoración que nos permita poder comparar los análisis realizados por separado. Con este objetivo, en MAGERIT v3 - Libro II - Catálogo de Elementos [10] (página 19) se sugiere el uso de unas escalas de valoración equivalentes (detallada y simplificada). Para el presente TFM, emplearemos la escala simplificada dado que se ha optado por realizar un análisis simple y no consumir demasiados recursos en el análisis.

En la siguiente tabla extraída de Magerit v3, se muestra la escala numérica con su equivalencia nominal que emplearemos en el TFM. Esta escala nos servirá para valorar como de grave será el

daño que sufrirá la empresa en el caso de que ese activo se pierda por completo. Cuanto más alto sea el valor en la escala, más grave resultara el daño que sufra la empresa.

Tabla 4. Escala de valoración de activos Magerit v3 – Libro II – Catalogo de elementos [10]



valor		**criterio**
10	(EX) extremo	Daño extremadamente grave
9	(MA) muy alto	Daño muy grave
6-8	(A) alto	Daño grave
3-5	(M) medio	Daño importante
1-2	(B) bajo	Daño menor
0	(MB) despreciable	Irrelevante a efectos prácticos

7.1.2. Ficha detalle de activos

Las fichas detalle de los activos consisten en fichas de catalogación propuestas en el apéndice 2 de Magerit v3 - Libro II – Catálogo de elementos [10]. En estas fichas, se expone toda la información disponible del activo, incluyendo una descripción, el propietario, el responsable, las valoraciones de las dimensiones y las posibles dependencias con otros activos.

Por comodidad, he decidido unir la tabla de información del activo con las tablas de valoración y dependencias del activo, para generar una ficha por cada activo.

Debida a la extensa longitud de las fichas en detalle para todos los activos del grupo empresarial, he dispuesto del "Anexo II - Inventario de activos – Fichas detalle" incluido en este TFM donde se incluyen todas las fichas en detalle de todos los activos categorizados.

A continuación se incluye un ejemplo del formato de la ficha de un activo tal y como se muestran en el Anexo II:

Tabla 5. Ejemplo de ficha detalle de un activo

Código: Formado por las siglas del tipo de activo y un número único por tipo	**Nombre:** Nombre asignado al activo
Descripción: Descripción del activo	
Propietario: Personal que hace del activo su propiedad	
Responsable: Personal responsable del activo	
Tipo: En el segundo libro de la metodología MAGERIT cada tipo activo se clasifica en subtipos del segundo libro de la Metodología Magerit – Catálogo de elementos.	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	Valor nominal	Justificación a la valoración de la dimensión de disponibilidad
[I]	Valor nominal	Justificación a la valoración de la dimensión de integridad
[C]	Valor nominal	Justificación a la valoración de la dimensión de confidencialidad
[A]	Valor nominal	Justificación a la valoración de la dimensión de autenticidad
[T]	Valor nominal	Justificación a la valoración de la dimensión de trazabilidad
Total	Valor nominal total	Justificación a la valoración total del activo

Dependencias de activos inferiores (hijos)	
Activo:	**¿Por qué?**

7.1.3. Catálogo general de activos

El catálogo general de activos consiste en una ficha resumen donde se muestran los activos de la empresa categorizados y una valoración total fruto de la suma de la valoración de todas las dimensiones del activo.

Tabla 6. Catálogo general de activos de Anónima S.L.

Tipo	Nombre	Código	Valor
[D] Datos / Información			
[files]	Documentación y planos de la producción	D001	MA
[files]	Archivo clientes	D002	EX
[password]	Datos acceso usuarios	D003	A
[password]	Datos acceso servidor	D004	MA
[backup]	Copias de seguridad	D005	A
[log]	Ficheros log	D006	A
[conf]	Ficheros configuración	D007	A
[int]	Base de datos del ERP	D008	MA
[int]	Base de datos del Gestor de proyectos	D009	MA
[files]	Datos personal empresa	D010	EX
[files]	Diseños	D011	M
[exe]	Mecanizados	D012	A
[K] Claves criptográficas			
[info][sign][public_signature]	Certificados empresa	K001	MA
[S] Servicios			
[email]	Email	S001	A
[www]	Web de la empresa	S002	M
[telnet]	VPN	S003	A
	Virtualización servidores	S004	A
	Cortafuegos	S005	M
	DHCP	S006	A
	DNS	S007	MA
	Servidor impresión	S008	M
[idm]	Active directory	S009	MA
[ipm]	GPO	S010	MA
	DNS caché	S011	B
	QUEQUES	S012	B
	WSUS	S013	M
[www]	Servidor web interno	S014	A

	Servidor ERP	S015	MA
	PostgreSQL	S016	MA
	Microsoft SQLServer	S017	MA
[SW] Software – Aplicaciones informáticas			
[std][office]	Paquete ofimático	SW001	M
[std][email_client]	Cliente de correo	SW002	A
[std][email_client]	Webmail	SW003	B
[std][browser]	Navegador Web	SW004	M
[std]	ERP (Microsoft Dynamics Navision 2017)	SW005	EX
[std]	Suite de diseño grafico	SW006	A
[std][av]	Antivirus	SW007	MA
[std][os]	Sistema operativo	SW008	MA
[std][backup]	Sistema de backup	SW009	A
[std]	Software gestión Wifi	SW010	B
[prp]	Software de fabricación	SW011	A
[prp]	Software de gestión de proyectos	SW012	MA
[std]	Wiki interna documentación	SW013	B
[std]	Software control inventario informático	SW014	A
[HW] Equipamiento informático (hardware)			
[pc]	Ordenadores oficina (40)	HW001	M
[mobile]	Ordenadores portátiles (15)	HW002	M
[mid]	Ordenadores diseño (15)	HW003	A
[mobile]	Tablets producción (20)	HW004	B
[pc]	Ordenadores producción (6)	HW005	B
[mid]	NAS (2)	HW006	MA
[network][router]	Router (1)	HW007	MA
[peripheral][print]	Impresoras (20)	HW008	M
[host]	Servidores físicos (3)	HW009	EX
[vhost]	Servidores virtualizados (12)	HW010	MA

[network][switch]	Switch (12)	HW011	A
[network]	Antenas enlace sedes (4)	HW012	EX
[network]	Antenas Wifi (12)	HW013	A
[network][switch]	Mini-switch (15)	HW014	MA
[peripheral][print]	Impresoras térmicas (20)	HW015	MB
[pc]	Terminales (20)	HW016	A
[mobile]	Autómatas (20)	HW017	A
[backup]	Servidor de copias	HW018	A
[COM] Redes de comunicaciones			
[LAN]	Red local	COM001	EX
[ADSL]	ADSL	COM002	B
[PSTN][mobile]	Servicio telefonía	COM003	MA
[wifi]	Wifi	COM004	M
[ISDN]	Fibra	COM005	MA
[pp]	Fibra oscura	COM006	MA
[MAN]	Enlaces antenas	COM007	EX
[Media] Soportes de información			
[electronic] [disk]	Discos duros extraíbles	MEDIA001	MA
[electronic] [dvd]	Blue-Ray	MEDIA002	A
[AUX] Equipamiento auxiliar			
	Lector huellas	AUX001	MB
	Cámaras seguridad	AUX002	A
[ups]	Sai	AUX003	M
[ac]	Equipo de climatización	AUX004	MA
[L] Instalaciones			
[building]	Nave principal	L001	MA
[building]	Almacén principal	L002	MA
[building]	Nave secundaria	L003	M
[building]	Almacén secundario	L004	M
[local]	CPD	L005	EX
[P] Personal			
[ui]	Gerencia	P001	EX
[ui]	Oficina	P002	MA

[ue]	Comerciales	P003	M
[adm][com][dba][sec][des]	Servicio informática	P004	MA
[op]	Operarios	P005	B

7.1.4. Selección de activos a analizar en detalle

Como comenté en los objetivos del TFM, no se va a realizar un análisis completo de todos los activos del grupo empresarial, ya que el objetivo del TFM es abordar todas las acciones necesarias, desde el análisis hasta el desarrollo de planes de contingencias y continuidad. Por lo tanto, procedo a realizar una selección de los activos que deben ser protegidos con mayor premura empleando la valoración dispuesta en el catálogo general de activos.

Además de basarme en el valor de los activos y en la comprobación de si ya cuentan con medidas de seguridad aplicadas (como el caso de las tablets en las que solo se permite acceder a las aplicaciones corporativas), también he realizado una entrevista con el responsable de informática de la empresa para asegurarme de que los activos seleccionados son contemplados como activos de gran valor por el personal responsable.

Por lo tanto, tras la selección realizada, el catálogo reducido de activos quedará así:

Tabla 7. Catálogo reducido de activos de Anónima S.L.

Tipo	Nombre	Código	Valor
[D] Datos / Información			
[files]	Documentación y planos de la producción	D001	MA
[files]	Archivo clientes	D002	EX
[backup]	Copias de seguridad	D005	A
[log]	Ficheros log	D006	A
[conf]	Ficheros configuración	D007	A
[int]	Base de datos del ERP	D008	MA
[int]	BD del Gestor de proyectos	D009	MA
[files]	Datos personal empresa	D010	EX
[S] Servicios			
[telnet]	VPN	S003	A
	Virtualización servidores	S004	A
	DNS	S007	MA

[idm]	Active directory	S009	MA
[ipm]	GPO	S010	MA
	Servidor ERP	S015	MA
	PostgreSQL	S016	MA
	Microsoft SQLServer	S017	MA
[SW] Software			
[std][email_client]	Cliente de correo	SW002	A
[std]	ERP (Microsoft Dynamics Navision 2017)	SW005	EX
[std]	Suite de diseño grafico	SW006	A
[std][av]	Antivirus	SW007	MA
[std][os]	Sistema operativo	SW008	MA
[std][backup]	Sistema de backup	SW009	A
[prp]	Software de fabricación	SW011	A
[prp]	Software de gestión de proyectos	SW012	MA
[HW] Hardware (equipamiento)			
[mid]	Ordenadores diseño (15)	HW003	A
[mid]	NAS (2)	HW006	MA
[network][router]	Router (1)	HW007	MA
[host]	Servidores físicos (3)	HW009	EX
[vhost]	Servidores virtualizados (12)	HW010	MA
[network][switch]	Switch (12)	HW011	A
[network][switch]	Mini-switch (15)	HW014	MA
[pc]	Terminales (20)	HW016	A
[backup]	Servidor de copias	HW018	A
[COM] Redes de comunicaciones			
[LAN]	Red local	COM001	EX
[ISDN]	Fibra	COM005	MA
[Media] Soportes de información			
[electronic] [disk]	Discos duros extraíbles	MEDIA001	MA
[electronic] [dvd]	Blue-Ray	MEDIA002	A
[L] Instalaciones			

[building]	Nave principal	L001	MA
[local]	CPD	L005	EX
[P] Personal			
[ui]	Gerencia	P001	EX
[ui]	Oficina	P002	MA

Tras el proceso de selección, los activos resultantes han sido clasificados de la siguiente manera:

- [D] Datos / Información: 8 activos.
- [S] Servicios: 8 activos.
- [SW] Software – Aplicaciones informáticas: 6 activos.
- [HW] Hardware – Equipamiento informático: 9 activos.
- [COM] Redes de comunicación: 2 activos.
- [Media] Soportes de información: 2 activos.
- [L] Instalaciones: 2 activos.
- [P] Personal: 2 activos.

7.2. Determinación de amenazas

En este paso se realizará la identificación y valoración de las amenazas a las que se pueden encontrar expuestas los activos y que pueden como resultado dañarlos en parte o de forma irreversible en cada una de sus dimensiones.

Tal y como se explicó en el capítulo 4.4.1. Método de análisis de riesgos Magerit v3, las amenazas pueden proceder de un origen diverso, tanto interno como externo a la organización (accidentes naturales, del entorno, fallos y vulnerabilidades en aplicaciones y equipamiento, accidentales o intencionadas causadas por personas).

Las amenazas según su tipo pueden afectar de una forma u otra a los distintos tipos de activos, por lo que se tendrá que identificar a que activos puede una amenaza afectar y sobre que dimensiones (disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad) esta amenaza se manifestará de mayor forma y con qué probabilidad podrá esta amenaza manifestarse.

Por lo tanto, necesitaremos identificar que activos se verán afectados por una amenaza, que nivel de degradación sufrirá en cada una de sus dimensiones por la acción de la amenaza y la probabilidad que existe de que esta amenaza ocurra. Para estimar la degradación se determina en qué medida perdería el valor el activo en caso de que ocurra la amenaza. Para estimar la probabilidad se estimará cual es la probabilidad de que se materialice.

Para realizar este análisis emplearemos una versión modificada de la plantilla para las fichas de amenaza ofrecida por Magerit v3 - Libro II – Catálogo de elementos [10] que adaptaremos para cada una de las amenazas.

Tabla 8. Plantilla de ficha amenazas de tipo [N.1] Amenaza de ejemplo (Fuente propia)

[N.1] Amenaza de ejemplo						
Tipos de activos afectados: [HW], [MEDIA], [AUX], [L]		**Dimensiones a las que afecta:** [D]				
Descripción: breve descripción de la amenaza						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[Código] Nombre de activo	MB	10	1	100		

Además, determinamos las escalas que emplearemos para determinar la frecuencia de ocurrencia y el nivel de degradación.

- La frecuencia de ocurrencia es la periodicidad con la que puede manifestarse determinada amenaza.

Tabla 9. Escala de probabilidad de materialización de amenazas (Fuente propia)

Código	Porcentaje	Descripción	Periodo
MA	100%	Muy frecuente	A diario
A	10%	Frecuente	Mensual
M	1%	Normal	Anual
B	0.1%	Poco frecuente	Cada varios años
MB	0.01%	Muy poco frecuente	Siglos

- El nivel de degradación es la cantidad porcentual de daño que la amenaza puede provocar sobre el activo.

Tabla 10. Escala de degradación del valor de un activo (Fuente propia)

Porcentaje	Descripción
100%	Irrecuperable
10%	Perceptible
1%	Inapreciable

7.2.1. [N] Desastres naturales

Tabla 11. Ficha de amenazas [N] Desastres naturales

[N] Desastres naturales						
Tipos de activos afectados: [HW], [MEDIA], [AUX], [L]		**Dimensiones a las que afecta:** [D]				
Descripción: posibilidad que el fuego, agua o un desastre natural acabe con los recursos del sistema						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	MB			100		
[HW006] NAS (2)	MB			100		
[HW007] Router	MB			100		
[HW009] Servidores físicos (3)	MB			100		
[HW010] Servidores virtualizados (12)	MB			100		
[HW011] Switch (12)	MB			100		
[HW014] Mini-switch (15)	MB			100		
[HW016] Terminales (20)	MB			100		
[HW018] Servidor de copias	MB			100		
[MEDIA001] Discos duros extraíbles	MB			100		
[MEDIA002] Blue-Ray	MB			100		
[L001] Nave principal	MB			100		
[L005] CPD	MB			100		

7.2.2. [I] De origen Industrial

Tabla 12. Ficha de amenazas [I.1] Fuego

[I.1] Fuego						
Tipos de activos afectados: [HW], [MEDIA], [AUX], [L]		**Dimensiones a las que afecta:** [D]				
Descripción: posibilidad que el fuego acabe con los recursos del sistema						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	B			100		
[HW006] NAS (2)	B			100		
[HW007] Router	B			100		
[HW009] Servidores físicos (3)	B			100		
[HW010] Servidores virtualizados (12)	B			100		
[HW011] Switch (12)	B			100		
[HW014] Mini-switch (15)	B			100		
[HW016] Terminales (20)	B			100		
[HW018] Servidor de copias	B			100		
[MEDIA001] Discos duros extraíbles	B			100		
[MEDIA002] Blue-Ray	B			100		
[L001] Nave principal	MB			100		
[L005] CPD	B			100		

Tabla 13. Ficha de amenazas [I.2] Daños por agua

[I.2] Daños por agua						
Tipos de activos afectados: [HW], [MEDIA], [AUX], [L]		**Dimensiones a las que afecta:** [D]				
Descripción: posibilidad que el agua acabe con los recursos del sistema						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	B			100		
[HW006] NAS (2)	B			100		
[HW007] Router	B			100		
[HW009] Servidores físicos (3)	B			100		
[HW010] Servidores virtualizados (12)	B			100		
[HW011] Switch (12)	B			100		
[HW014] Mini-switch (15)	B			100		
[HW016] Terminales (20)	B			100		
[HW018] Servidor de copias	B			100		
[MEDIA001] Discos duros extraíbles	B			100		
[MEDIA002] Blue-Ray	B			100		
[L001] Nave principal	B			10		
[L005] CPD	MB			10		

Tabla 14. Ficha de amenazas [I.] Desastres naturales*

[I.*] Desastres naturales						
Tipos de activos afectados: [HW], [MEDIA], [AUX], [L]		**Dimensiones a las que afecta:** [D]				
Descripción: posibilidad que el fuego acabe con los recursos del sistema						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	MB			100		
[HW006] NAS (2)	MB			100		
[HW007] Router	MB			100		
[HW009] Servidores físicos (3)	MB			100		
[HW010] Servidores virtualizados (12)	MB			100		
[HW011] Switch (12)	MB			100		
[HW014] Mini-switch (15)	MB			100		
[HW016] Terminales (20)	MB			100		
[HW018] Servidor de copias	MB			100		
[MEDIA001] Discos duros extraíbles	MB			100		
[MEDIA002] Blue-Ray	MB			100		
[L001] Nave principal	MB			10		
[L005] CPD	MB			10		

Tabla 15. Ficha de amenazas [I.3] Contaminación mecánica

[I.3] Contaminación mecánica						
Tipos de activos afectados: [HW], [MEDIA], [AUX]		**Dimensiones a las que afecta:** [D]				
Descripción: posibilidad que vibraciones, polvo o suciedad acaben con los recursos del sistema						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	M			10		
[HW006] NAS (2)	M			10		
[HW007] Router	M			10		
[HW009] Servidores físicos (3)	M			10		
[HW010] Servidores virtualizados (12)	M			10		
[HW011] Switch (12)	B			10		
[HW014] Mini-switch (15)	M			10		
[HW016] Terminales (20)	M			100		
[HW018] Servidor de copias	M			10		
[MEDIA001] Discos duros extraíbles	M			10		
[MEDIA002] Blue-Ray	M			100		

Tabla 16. Ficha de amenazas [I.4] Contaminación electromagnética

[I.4] Contaminación electromagnética						
Tipos de activos afectados: [HW], [MEDIA], [AUX]		**Dimensiones a las que afecta:** [D]				
Descripción: posibilidad que interferencias de radio, campos magnéticos, luz ultra afecten al sistema						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	MB			10		
[HW006] NAS (2)	MB			10		
[HW007] Router	B			10		
[HW009] Servidores físicos (3)	MB			10		
[HW010] Servidores virtualizados (12)	MB			10		
[HW011] Switch (12)	B			10		
[HW014] Mini-switch (15)	B			10		
[HW016] Terminales (20)	MB			10		
[HW018] Servidor de copias	MB			10		
[MEDIA001] Discos duros extraíbles	MB			100		
[MEDIA002] Blue-Ray	MB			100		

Tabla 17. Ficha de amenazas [I.5] Avería de origen físico o lógico

[I.5] Avería de origen físico o lógico						
Tipos de activos afectados: [SW], [HW], [MEDIA], [AUX]		**Dimensiones a las que afecta:** [D]				
Descripción: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[SW002] Cliente de correo	MB			10		
[SW005] ERP	B			10		
[SW006] Suite de diseño grafico	B			10		
[SW007] Antivirus	MB			10		
[SW008] Sistema operativo	B			10		
[SW009] Sistema de backup	MB			10		
[SW011] Software de fabricación	MB			10		
[SW012] Software de gestión de proyectos	MB			10		
[HW003] Ordenadores diseño (15)	B			100		
[HW006] NAS (2)	B			100		
[HW007] Router	B			100		
[HW009] Servidores físicos (3)	M			100		
[HW010] Servidores virtualizados (12)	M			10		
[HW011] Switch (12)	B			100		
[HW014] Mini-switch (15)	B			100		
[HW016] Terminales (20)	MB			100		
[HW018] Servidor de copias	MB			100		
[MEDIA001] Discos duros extraíbles	MB			100		
[MEDIA002] Blue-Ray	MB			100		

Tabla 18. Ficha de amenazas [I.6] Corte de suministro eléctrico

[I.6] Corte de suministro eléctrico						
Tipos de activos afectados: [HW], [MEDIA], [AUX]		**Dimensiones a las que afecta:** [D]				
Descripción: cese en la alimentación de potencia.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	MB			100		
[HW006] NAS (2)	MB			100		
[HW007] Router	MB			100		
[HW009] Servidores físicos (3)	MB			100		
[HW010] Servidores virtualizados (12)	MB			100		
[HW011] Switch (12)	MB			100		
[HW014] Mini-switch (15)	MB			100		
[HW016] Terminales (20)	MB			100		
[HW018] Servidor de copias	MB			100		
[MEDIA001] Discos duros extraíbles	MB			100		
[MEDIA002] Blue-Ray	MB			100		

Tabla 19. Ficha de amenazas [I.7] Condiciones inadecuadas de temperatura o humedad

[I.7] Condiciones inadecuadas de temperatura o humedad						
Tipos de activos afectados: [HW], [MEDIA], [AUX]		**Dimensiones a las que afecta:** [D]				
Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad…						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	B			10		
[HW006] NAS (2)	B			10		
[HW007] Router	B			100		
[HW009] Servidores físicos (3)	M			10		
[HW010] Servidores virtualizados (12)	M			10		
[HW011] Switch (12)	B			100		
[HW014] Mini-switch (15)	B			10		
[HW016] Terminales (20)	MB			100		
[HW018] Servidor de copias	B			10		
[MEDIA001] Discos duros extraíbles	MB			10		
[MEDIA002] Blue-Ray	MB			100		

Tabla 20. Ficha de amenazas [I.8] Fallo de servicios de comunicaciones

[I.8] Fallo de servicios de comunicaciones						
Tipos de activos afectados: [COM]		**Dimensiones a las que afecta:** [D]				
Descripción: cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[COM001] Red local LAN	MB			100		
[COM005] Fibra	MB			100		

Tabla 21. Ficha de amenazas [I.10] Degradación de los soportes de almacenamiento de la información

[I.10] Degradación de los soportes de almacenamiento de la información						
Tipos de activos afectados: [MEDIA]		**Dimensiones a las que afecta:** [D]				
Descripción: Degradación de los soportes de almacenamiento consecuencia del paso del tiempo						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[MEDIA001] Discos duros extraíbles	MB			10		
[MEDIA002] Blue-Ray	B			10		

Tabla 22. Ficha de amenazas [I.11] Emanaciones electromagnéticas

[I.11] Emanaciones electromagnéticas						
Tipos de activos afectados: [HW], [MEDIA], [AUX], [L]		**Dimensiones a las que afecta:** [D]				
Descripción: hecho de poner vía radio datos internos a disposición de terceros.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	MB			1		
[HW006] NAS (2)	MB			1		
[HW007] Router	MB			1		
[HW009] Servidores físicos (3)	MB			1		
[HW010] Servidores virtualizados (12)	MB			1		
[HW011] Switch (12)	MB			1		
[HW014] Mini-switch (15)	MB			1		
[HW016] Terminales (20)	MB			1		
[HW018] Servidor de copias	MB			1		
[MEDIA001] Discos duros extraíbles	MB			1		
[MEDIA002] Blue-Ray	MB			1		
[L001] Nave principal	MB			1		
[L005] CPD	MB			1		

7.2.3. [E] Errores y fallos no intencionados

Tabla 23. Ficha de amenazas [E.1] Errores y fallos no intencionados

[E.1] Errores de los usuarios						
Tipos de activos afectados: [D], [KEYS], [S], [SW], [MEDIA]		**Dimensiones a las que afecta:** [I], [C], [D]				
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D001] Documentación y planos de la producción	A	10	10	10		
[D002] Archivo clientes	M	10	10	1		
[D005] Copias de seguridad	MB	1	1	1		
[D006] Ficheros log	MB	1	1	1		
[D007] Ficheros configuración	MB	1	1	1		
[D008] Base de datos del ERP	MB	1	1	1		
[D009] BD del Gestor de proyectos	MB	1	1	1		
[D010] Datos personal empresa	M	10	10	1		
[S003] VPN	MB	1	1	1		
[S004] Virtualización servidores	MB	1	1	1		
[S007] DNS	MB	1	1	1		
[S009] Active directory	MB	1	1	1		
[S010] GPO	MB	1	1	1		
[S015] Servidor ERP	MB	1	1	1		
[S016] PostgreSQL	MB	1	1	1		
[S017] Microsoft SQLServer	MB	1	1	1		
[SW002] Cliente de correo	B	1	1	10		
[SW005] ERP (Microsoft Dynamics Navision 2017)	MA	10	100	1		
[SW006] Suite de diseño grafico	M	10	10	10		

[SW007] Antivirus	MB	1	1	1		
[SW008] Sistema operativo	B	1	1	1		
[SW009] Sistema de backup	MB	1	1	1		
[SW011] Software de fabricación	A	10	1	1		
[SW012] Software de gestión de proyectos	A	10	1	1		
[MEDIA001] Discos duros extraíbles	MB	10	100	10		
[MEDIA002] Blue-Ray	MB	10	100	10		

Tabla 24. Ficha de amenazas [E.2] Errores del administrador

[E.2] Errores del administrador						
Tipos de activos afectados: [D], [KEYS], [S], [SW], [HW], [COM], [MEDIA]		**Dimensiones a las que afecta:** [D], [I], [C]				
Descripción: equivocaciones de personas con responsabilidades de instalación y operación.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D001] Documentación y planos de la producción	MB	10	10	10		
[D002] Archivo clientes	MB	10	10	10		
[D005] Copias de seguridad	M	100	10	10		
[D006] Ficheros log	MB	10	10	10		
[D007] Ficheros configuración	M	10	10	10		
[D008] Base de datos del ERP	M	10	10	10		
[D009] BD del Gestor de proyectos	M	100	10	10		
[D010] Datos personal empresa	MB	10	10	10		
[S003] VPN	B	1	1	10		
[S004] Virtualización servidores	B	10	1	10		
[S007] DNS	B	1	1	10		
[S009] Active directory	B	10	1	1		
[S010] GPO	B	1	1	10		

[S015] Servidor ERP	M	1	1	10		
[S016] PostgreSQL	B	1	1	10		
[S017] Microsoft SQLServer	B	1	1	10		
[SW002] Cliente de correo	B	1	1	10		
[SW005] ERP (Microsoft Dynamics Navision 2017)	B	1	10	10		
[SW006] Suite de diseño grafico	MB	1	1	1		
[SW007] Antivirus	MB	1	1	1		
[SW008] Sistema operativo	MB	1	1	1		
[SW009] Sistema de backup	MB	1	1	1		
[SW011] Software de fabricación	M	1	1	10		
[SW012] Software de gestión de proyectos	M	1	1	10		
[HW003] Ordenadores diseño (15)	MB	1	10	10		
[HW006] NAS (2)	MB	1	1	10		
[HW007] Router	B	10	10	10		
[HW009] Servidores físicos (3)	B	10	10	10		
[HW010] Servidores virtualizados (12)	M	10	10	0		
[HW011] Switch (12)	MB	1	1	10		
[HW014] Mini-switch (15)	B	1	1	10		
[HW016] Terminales (20)	MB	1	1	1		
[HW018] Servidor de copias	MB	10	100	10		
[COM001] Red local LAN	B	10	10	10		
[COM005] Fibra	MB	1	1	1		
[MEDIA001] Discos duros extraíbles	MB	10	100	100		
[MEDIA002] Blue-Ray	MB	10	100	10		

Tabla 25. Ficha de amenazas [E.3] Errores de monitorización (log)

[E.3] Errores de monitorización (log)						
Tipos de activos afectados: [D.LOG]		**Dimensiones a las que afecta:** [I], [C]				
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ...						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D006] Ficheros log	M	10				10

Tabla 26. Ficha de amenazas [E.4] Errores de configuración

[E.4] Errores de configuración						
Tipos de activos afectados: [D.CONF]		**Dimensiones a las que afecta:** [I], [C]				
Descripción: introducción de datos de configuración erróneos.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D007] Ficheros configuración	B	10	10			

Tabla 27. Ficha de amenazas [E.8] Difusión de software dañino

[E.8] Difusión de software dañino						
Tipos de activos afectados: [SW]		**Dimensiones a las que afecta:** [D], [I], [C]				
Descripción: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[SW002] Cliente de correo	B	10	100	10		
[SW005] ERP (Microsoft Dynamics Navision 2017)	MB	100	100	100		

[SW006] Suite de diseño grafico	MB	10	1	10		
[SW007] Antivirus	MB	10	1	10		
[SW008] Sistema operativo	B	10	100	10		
[SW009] Sistema de backup	MB	10	10	10		
[SW011] Software de fabricación	MB	10	10	10		
[SW012] Software de gestión de proyectos	MB	10	100	10		

Tabla 28. Ficha de amenazas [E.9] Errores de [re-]encaminamiento

[E.9] Errores de [re-]encaminamiento						
Tipos de activos afectados: [S], [SW], [COM]		**Dimensiones a las que afecta:** [C]				
Descripción: envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[S003] VPN	MB		100			
[S004] Virtualización servidores	MB		1			
[S007] DNS	MB		100			
[S009] Active directory	MB		10			
[S010] GPO	MB		10			
[S015] Servidor ERP	MB		100			
[S016] PostgreSQL	MB		100			
[S017] Microsoft SQLServer	MB		100			
[SW002] Cliente de correo	MB		10			
[SW005] ERP (Microsoft Dynamics Navision 2017)	MB		10			
[SW006] Suite de diseño grafico	MB		1			
[SW007] Antivirus	MB		1			

[SW008] Sistema operativo	MB		10			
[SW009] Sistema de backup	MB		1			
[SW011] Software de fabricación	MB		1			
[SW012] Software de gestión de proyectos	MB		10			
[COM001] Red local LAN	MB		100			
[COM005] Fibra	MB		100			

Tabla 29. Ficha de amenazas [E.10] Errores de secuencia

[E.10] Errores de secuencia						
Tipos de activos afectados: [S], [SW], [COM]		**Dimensiones a las que afecta:** [I]				
Descripción: alteración accidental del orden de los mensajes transmitidos.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[S003] VPN	MB	1				
[S004] Virtualización servidores	MB	1				
[S007] DNS	MB	1				
[S009] Active directory	MB	1				
[S010] GPO	MB	1				
[S015] Servidor ERP	MB	1				
[S016] PostgreSQL	MB	1				
[S017] Microsoft SQLServer	MB	1				
[SW002] Cliente de correo	MB	1				
[SW005] ERP (Microsoft Dynamics Navision 2017)	MB	1				
[SW006] Suite de diseño grafico	MB	1				
[SW007] Antivirus	MB	1				
[SW008] Sistema operativo	MB	1				
[SW009] Sistema de backup	MB	1				

[SW011] Software de fabricación	MB	1				
[SW012] Software de gestión de proyectos	MB	1				
[COM001] Red local LAN	MB	10				
[COM005] Fibra	MB	10				

Tabla 30. Ficha de amenazas [E.15] Alteración accidental de la información

[E.15] Alteración accidental de la información						
Tipos de activos afectados: [D], [KEYS], [S], [SW], [COM], [MEDIA], [L]	**Dimensiones a las que afecta:** [I]					
Descripción: alteración accidental de la información.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D001] Documentación y planos de la producción	M	10				
[D002] Archivo clientes	M	10				
[D005] Copias de seguridad	MB	1				
[D006] Ficheros log	MB	1				
[D007] Ficheros configuración	B	10				
[D008] Base de datos del ERP	MB	1				
[D009] BD del Gestor de proyectos	B	1				
[D010] Datos personal empresa	M	10				
[S003] VPN	MB	10				
[S004] Virtualización servidores	MB	10				
[S007] DNS	MB	1				
[S009] Active directory	MB	1				
[S010] GPO	MB	1				
[S015] Servidor ERP	MB	10				
[S016] PostgreSQL	M	10				
[S017] Microsoft SQLServer	M	10				

[SW002] Cliente de correo	B	1				
[SW005] ERP (Microsoft Dynamics Navision 2017)	B	10				
[SW006] Suite de diseño grafico	MB	10				
[SW007] Antivirus	MB	1				
[SW008] Sistema operativo	MB	1				
[SW009] Sistema de backup	B	1				
[SW011] Software de fabricación	A	10				
[SW012] Software de gestión de proyectos	M	10				
[COM001] Red local LAN	MB	1				
[COM005] Fibra	MB	1				
[MEDIA001] Discos duros extraíbles	B	10				
[MEDIA002] Blue-Ray	B	100				
[L001] Nave principal	MB	100				
[L005] CPD	MB	10				

Tabla 31. Ficha de amenazas [E.18] Destrucción de la información

[E.18] Destrucción de la información						
Tipos de activos afectados: [D], [KEYS], [S], [SW], [COM], [MEDIA], [L]	**Dimensiones a las que afecta:** [D], [I]					
Descripción: perdida accidental de la información.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D001] Documentación y planos de la producción	M			100		
[D002] Archivo clientes	B			100		
[D005] Copias de seguridad	MB			100		
[D006] Ficheros log	B			10		
[D007] Ficheros configuración	B			100		
[D008] Base de datos del ERP	B			100		

[D009] BD del Gestor de proyectos	B			100		
[D010] Datos personal empresa	B			100		
[S003] VPN	MB			1		
[S004] Virtualización servidores	MB			1		
[S007] DNS	MB			1		
[S009] Active directory	MB			10		
[S010] GPO	MB			10		
[S015] Servidor ERP	MB			1		
[S016] PostgreSQL	B			100		
[S017] Microsoft SQLServer	B			100		
[SW002] Cliente de correo	MB			10		
[SW005] ERP (Microsoft Dynamics Navision 2017)	MB			100		
[SW006] Suite de diseño grafico	MB			10		
[SW007] Antivirus	MB			10		
[SW008] Sistema operativo	MB			10		
[SW009] Sistema de backup	MB			10		
[SW011] Software de fabricación	MB			1		
[SW012] Software de gestión de proyectos	M			10		
[COM001] Red local LAN	MB			1		
[COM005] Fibra	MB			1		
[MEDIA001] Discos duros extraíbles	B			100		
[MEDIA002] Blue-Ray	MB			100		
[L001] Nave principal	B			100		
[L005] CPD	B			100		

Tabla 32. Ficha de amenazas [E.19] Fugas de información

[E.19] Fugas de información						
Tipos de activos afectados: [D], [KEYS], [S], [SW], [COM], [MEDIA], [L], [P]		**Dimensiones a las que afecta:** [C]				
Descripción: revelación por indiscreción.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D001] Documentación y planos de la producción	B		100			
[D002] Archivo clientes	MB		10			
[D005] Copias de seguridad	MB		1			
[D006] Ficheros log	MB		1			
[D007] Ficheros configuración	MB		10			
[D008] Base de datos del ERP	MB		1			
[D009] BD del Gestor de proyectos	MB		1			
[D010] Datos personal empresa	B		10			
[S003] VPN	MB		1			
[S004] Virtualización servidores	MB		1			
[S007] DNS	MB		1			
[S009] Active directory	MB		1			
[S010] GPO	MB		1			
[S015] Servidor ERP	MB		1			
[S016] PostgreSQL	MB		1			
[S017] Microsoft SQLServer	MB		1			
[SW002] Cliente de correo	M		100			
[SW005] ERP (Microsoft Dynamics Navision 2017)	MB		100			
[SW006] Suite de diseño grafico	MB		1			
[SW007] Antivirus	MB		1			
[SW008] Sistema operativo	MB		1			

[SW009] Sistema de backup	MB		1			
[SW011] Software de fabricación	MB		1			
[SW012] Software de gestión de proyectos	MB		10			
[COM001] Red local LAN	MB		10			
[COM005] Fibra	MB		10			
[MEDIA001] Discos duros extraíbles	MB		100			
[MEDIA002] Blue-Ray	B		100			
[L001] Nave principal	M		10			
[L005] CPD	B		10			
[P001] Gerencia	M		100			
[P002] Oficina	M		100			

Tabla 33. Ficha de amenazas [E.20] Vulnerabilidades de los programas (software)

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos afectados: [SW]	**Dimensiones a las que afecta:** [I], [D], [C]
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	

Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[SW002] Cliente de correo	MB	10	100	10		
[SW005] ERP (Microsoft Dynamics Navision 2017)	B	10	100	10		
[SW006] Suite de diseño grafico	B	10	10	10		
[SW007] Antivirus	MB	100	10	10		
[SW008] Sistema operativo	B	1	100	1		
[SW009] Sistema de backup	B	10	100	10		
[SW011] Software de fabricación	M	10	1	10		
[SW012] Software de gestión de proyectos	M	10	10	10		

Tabla 34. Ficha de amenazas [E.21] Errores de mantenimiento / actualización de programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)						
Tipos de activos afectados: [SW]		**Dimensiones a las que afecta:** [I], [D], [C]				
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[SW002] Cliente de correo	MB	10	10	10		
[SW005] ERP (Microsoft Dynamics Navision 2017)	B	10	10	10		
[SW006] Suite de diseño grafico	B	10	1	10		
[SW007] Antivirus	MB	100	1	10		
[SW008] Sistema operativo	B	1	1	1		
[SW009] Sistema de backup	B	10	1	10		
[SW011] Software de fabricación	M	10	1	10		
[SW012] Software de gestión de proyectos	M	10	10	10		

Tabla 35. Ficha de amenazas [E.23] Errores de mantenimiento / actualización de equipos (hardware)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)						
Tipos de activos afectados: [HW], [MEDIA], [AUX]		**Dimensiones a las que afecta:** [D]				
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	B			10		
[HW006] NAS (2)	B			10		
[HW007] Router	B			10		
[HW009] Servidores físicos (3)	B			10		

[HW010] Servidores virtualizados (12)	M			10		
[HW011] Switch (12)	MB			10		
[HW014] Mini-switch (15)	B			10		
[HW016] Terminales (20)	B			10		
[HW018] Servidor de copias	MB			10		
[MEDIA001] Discos duros extraíbles	B			10		
[MEDIA002] Blue-Ray	MB			10		

Tabla 36. Ficha de amenazas [E.24] Caída del sistema por agotamiento de recursos

[E.24] Caída del sistema por agotamiento de recursos						
Tipos de activos afectados: [S], [HW], [COM]		**Dimensiones a las que afecta:** [D]				
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[S003] VPN	B			10		
[S004] Virtualización servidores	B			10		
[S007] DNS	MB			1		
[S009] Active directory	MB			1		
[S010] GPO	MB			1		
[S015] Servidor ERP	B			1		
[S016] PostgreSQL	B			10		
[S017] Microsoft SQLServer	B			10		
[HW003] Ordenadores diseño (15)	B			1		
[HW006] NAS (2)	B			10		
[HW007] Router	B			10		
[HW009] Servidores físicos (3)	B			10		
[HW010] Servidores virtualizados (12)	B			10		

[HW011] Switch (12)	B			10		
[HW014] Mini-switch (15)	B			100		
[HW016] Terminales (20)	MB			1		
[HW018] Servidor de copias	B			10		
[COM001] Red local LAN	B			100		
[COM005] Fibra	B			100		

Tabla 37. Ficha de amenazas [E.25] Perdida de equipos

[E.25] Perdida de equipos						
Tipos de activos afectados: [HW], [MEDIA], [AUX]		**Dimensiones a las que afecta:** [D], [C]				
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	MB		100	100		
[HW006] NAS (2)	MB		100	100		
[HW007] Router	MB		10	100		
[HW009] Servidores físicos (3)	MB		100	100		
[HW010] Servidores virtualizados (12)	MB		1	1		
[HW011] Switch (12)	MB		1	100		
[HW014] Mini-switch (15)	B		1	100		
[HW016] Terminales (20)	MB		100	10		
[HW018] Servidor de copias	MB		100	100		
[MEDIA001] Discos duros extraíbles	B		100	100		
[MEDIA002] Blue-Ray	B		100	100		

Tabla 38. Ficha de amenazas [E.28] Indisponibilidad del personal

[E.28] Indisponibilidad del personal						
Tipos de activos afectados: [P]		**Dimensiones a las que afecta:** [D]				
Descripción: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ...						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[P001] Gerencia	M			100		
[P002] Oficina	M			100		

7.2.4. [A] Ataques intencionados

Tabla 39. Ficha de amenazas [A.3] Manipulación de los registros de actividad (log)

[A.3] Manipulación de los registros de actividad (log)						
Tipos de activos afectados: [D.LOG]		**Dimensiones a las que afecta:** [I], [T]				
Descripción: manipulación registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ...						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D006] Ficheros log	MB	10				10

Tabla 40. Ficha de amenazas [A.4] Manipulación de la configuración

[A.4] Manipulación de la configuración						
Tipos de activos afectados: [D.CONF]		**Dimensiones a las que afecta:** [I], [C], [A]				
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D007] Ficheros configuración	MB	100	100		100	

Tabla 41. Ficha de amenazas [A.5] Suplantación de la identidad del usuario

[A.5] Suplantación de la identidad del usuario						
Tipos de activos afectados: [D], [KEYS], [S], [SW], [COM]		**Dimensiones a las que afecta:** [C], [A], [I]				
Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D001] Documentación y planos de la producción	B	10	100		10	
[D002] Archivo clientes	B	10	100		10	
[D005] Copias de seguridad	MB	10	100		10	
[D006] Ficheros log	MB	10	100		10	
[D007] Ficheros configuración	MB	10	100		10	
[D008] Base de datos del ERP	MB	10	100		10	
[D009] BD del Gestor de proyectos	MB	10	100		10	
[D010] Datos personal empresa	B	10	100		10	
[S003] VPN	B	1	10		100	
[S004] Virtualización servidores	MB	1	100		10	
[S007] DNS	MB	1	100		100	

[S009] Active directory	MB	1	100		100	
[S010] GPO	MB	1	10		100	
[S015] Servidor ERP	MB	1	10		100	
[S016] PostgreSQL	MB	1	100		100	
[S017] Microsoft SQLServer	MB	1	100		100	
[SW002] Cliente de correo	MB	10	100		100	
[SW005] ERP (Microsoft Dynamics Navision 2017)	MB	10	100		100	
[SW006] Suite de diseño grafico	MB	1	10		100	
[SW007] Antivirus	MB	10	10		100	
[SW008] Sistema operativo	B	1	100		100	
[SW009] Sistema de backup	MB	10	10		100	
[SW011] Software de fabricación	MB	10	100		100	
[SW012] Software de gestión de proyectos	B	10	10		100	
[COM001] Red local LAN	B	10	100		100	
[COM005] Fibra	MB	10	100		100	

Tabla 42. Ficha de amenazas [A.6] Abuso de privilegios de acceso

[A.6] Abuso de privilegios de acceso	
Tipos de activos afectados: [D], [KEYS], [S], [SW], [HW], [COM]	**Dimensiones a las que afecta:** [C], [I], [D]
Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	

Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D001] Documentación y planos de la producción	A	10	100	10		
[D002] Archivo clientes	M	10	100	10		
[D005] Copias de seguridad	MB	10	10	10		

[D006] Ficheros log	MB	10	10	10		
[D007] Ficheros configuración	MB	10	10	10		
[D008] Base de datos del ERP	MB	10	10	10		
[D009] BD del Gestor de proyectos	MB	10	10	10		
[D010] Datos personal empresa	M	10	100	10		
[S003] VPN	MB	1	1	1		
[S004] Virtualización servidores	MB	1	1	1		
[S007] DNS	MB	1	1	10		
[S009] Active directory	MB	1	10	10		
[S010] GPO	MB	1	10	10		
[S015] Servidor ERP	MB	1	1	1		
[S016] PostgreSQL	MB	1	10	10		
[S017] Microsoft SQLServer	MB	1	10	10		
[SW002] Cliente de correo	MB	10	10	1		
[SW005] ERP (Microsoft Dynamics Navision 2017)	A	10	100	10		
[SW006] Suite de diseño grafico	MB	10	10	10		
[SW007] Antivirus	MB	100	10	10		
[SW008] Sistema operativo	B	1	10	1		
[SW009] Sistema de backup	MB	10	100	10		
[SW011] Software de fabricación	B	10	10	10		
[SW012] Software de gestión de proyectos	A	10	100	10		
[HW003] Ordenadores diseño (15)	M	10	10	10		
[HW006] NAS (2)	B	10	100	10		
[HW007] Router	B	100	100	10		
[HW009] Servidores físicos (3)	B	10	100	10		
[HW010] Servidores virtualizados (12)	MB	10	100	10		
[HW011] Switch (12)	B	10	100	10		
[HW014] Mini-switch (15)	B	10	100	10		

[HW016] Terminales (20)	MB	10	10	10		
[HW018] Servidor de copias	MB	10	100	10		
[COM001] Red local LAN	M	10	100	10		
[COM005] Fibra	MB	1	100	1		

Tabla 43. Ficha de amenazas [A.7] Uso no previsto

[A.7] Uso no previsto						
Tipos de activos afectados: [S], [SW], [HW], [COM], [MEDIA], [AUX], [L]		**Dimensiones a las que afecta:** [D], [C], [I]				
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[S003] VPN	MB	10	10	10		
[S004] Virtualización servidores	MB	10	10	10		
[S007] DNS	MB	10	10	10		
[S009] Active directory	MB	10	10	10		
[S010] GPO	MB	10	10	10		
[S015] Servidor ERP	MB	10	10	10		
[S016] PostgreSQL	MB	10	10	10		
[S017] Microsoft SQLServer	MB	10	10	10		
[SW002] Cliente de correo	B	10	100	10		
[SW005] ERP (Microsoft Dynamics Navision 2017)	B	10	10	10		
[SW006] Suite de diseño grafico	B	10	10	100		
[SW007] Antivirus	MB	10	10	10		
[SW008] Sistema operativo	B	10	100	10		
[SW009] Sistema de backup	MB	10	100	10		

[SW011] Software de fabricación	MB	10	10	10		
[SW012] Software de gestión de proyectos	MB	10	100	10		
[HW003] Ordenadores diseño (15)	M	10	10	10		
[HW006] NAS (2)	MB	10	100	10		
[HW007] Router	MB	10	100	10		
[HW009] Servidores físicos (3)	MB	10	100	10		
[HW010] Servidores virtualizados (12)	MB	10	100	10		
[HW011] Switch (12)	B	10	100	10		
[HW014] Mini-switch (15)	M	10	100	10		
[HW016] Terminales (20)	MB	10	10	10		
[HW018] Servidor de copias	MB	10	100	10		
[COM001] Red local LAN	B	10	100	10		
[COM005] Fibra	MB	10	100	10		
[MEDIA001] Discos duros extraíbles	MB	100	100	100		
[MEDIA002] Blue-Ray	MB	100	100	100		
[L001] Nave principal	MB	10	10	10		
[L005] CPD	B	10	10	10		

Tabla 44. Ficha de amenazas [A.8] Difusión de software dañino

[A.8] Difusión de software dañino						
Tipos de activos afectados: [SW]		**Dimensiones a las que afecta:** [D], [I], [C]				
Descripción: propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[SW002] Cliente de correo	MB	10	100	10		
[SW005] ERP (Microsoft Dynamics Navision 2017)	MB	100	100	100		

[SW006] Suite de diseño grafico	MB	10	1	10		
[SW007] Antivirus	MB	10	1	10		
[SW008] Sistema operativo	MB	10	100	10		
[SW009] Sistema de backup	MB	10	100	100		
[SW011] Software de fabricación	MB	10	10	100		
[SW012] Software de gestión de proyectos	MB	10	100	100		

Tabla 45. Ficha de amenazas [A.9] [Re-]encaminamiento de mensajes

[A.9] [Re-]encaminamiento de mensajes						
Tipos de activos afectados: [S], [SW], [COM]		**Dimensiones a las que afecta:** [C]				
Descripción: envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[S003] VPN	MB		100			
[S004] Virtualización servidores	MB		10			
[S007] DNS	MB		100			
[S009] Active directory	MB		10			
[S010] GPO	MB		10			
[S015] Servidor ERP	MB		10			
[S016] PostgreSQL	MB		100			
[S017] Microsoft SQLServer	MB		100			
[SW002] Cliente de correo	MB		10			
[SW005] ERP (Microsoft Dynamics Navision 2017)	MB		1			
[SW006] Suite de diseño grafico	MB		1			
[SW007] Antivirus	MB		1			

[SW008] Sistema operativo	MB		10			
[SW009] Sistema de backup	MB		1			
[SW011] Software de fabricación	MB		10			
[SW012] Software de gestión de proyectos	MB		100			
[COM001] Red local LAN	B		100			
[COM005] Fibra	MB		100			

Tabla 46. Ficha de amenazas [A.10] Alteración de secuencia

[A.10] Alteración de secuencia						
Tipos de activos afectados: [S], [SW], [COM]		**Dimensiones a las que afecta:** [I]				
Descripción: alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[S003] VPN	MB	1				
[S004] Virtualización servidores	MB	1				
[S007] DNS	MB	1				
[S009] Active directory	MB	1				
[S010] GPO	MB	1				
[S015] Servidor ERP	MB	1				
[S016] PostgreSQL	MB	1				
[S017] Microsoft SQLServer	MB	1				
[SW002] Cliente de correo	MB	1				
[SW005] ERP (Microsoft Dynamics Navision 2017)	MB	1				
[SW006] Suite de diseño grafico	MB	1				
[SW007] Antivirus	MB	1				
[SW008] Sistema operativo	MB	1				

[SW009] Sistema de backup	MB	1				
[SW011] Software de fabricación	MB	1				
[SW012] Software de gestión de proyectos	MB	1				
[COM001] Red local LAN	B	10				
[COM005] Fibra	MB	10				

Tabla 47. Ficha de amenazas [A.11] Acceso no autorizado

[A.11] Acceso no autorizado						
Tipos de activos afectados: [D], [KEYS], [S], [SW], [HW], [COM], [MEDIA], [AUX], [L]		**Dimensiones a las que afecta:** [C], [I]				
Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D001] Documentación y planos de la producción	B	10	100			
[D002] Archivo clientes	B	10	100			
[D005] Copias de seguridad	MB	10	100			
[D006] Ficheros log	MB	10	100			
[D007] Ficheros configuración	MB	10	100			
[D008] Base de datos del ERP	MB	10	100			
[D009] BD del Gestor de proyectos	MB	10	100			
[D010] Datos personal empresa	B	10	100			
[S003] VPN	MB	10	100			
[S004] Virtualización servidores	MB	10	100			
[S007] DNS	MB	10	100			
[S009] Active directory	MB	10	100			
[S010] GPO	MB	10	100			
[S015] Servidor ERP	MB	10	100			

[S016] PostgreSQL	B	10	100			
[S017] Microsoft SQLServer	B	10	100			
[SW002] Cliente de correo	MB	10	100			
[SW005] ERP (Microsoft Dynamics Navision 2017)	B	10	100			
[SW006] Suite de diseño grafico	MB	10	10			
[SW007] Antivirus	MB	100	10			
[SW008] Sistema operativo	B	10	100			
[SW009] Sistema de backup	MB	10	100			
[SW011] Software de fabricación	MB	10	10			
[SW012] Software de gestión de proyectos	MB	10	100			
[HW003] Ordenadores diseño (15)	M	10	10			
[HW006] NAS (2)	B	10	10			
[HW007] Router	B	10	100			
[HW009] Servidores físicos (3)	B	10	10			
[HW010] Servidores virtualizados (12)	B	10	10			
[HW011] Switch (12)	B	10	100			
[HW014] Mini-switch (15)	B	10	100			
[HW016] Terminales (20)	B	10	10			
[HW018] Servidor de copias	B	10	10			
[COM001] Red local LAN	M	10	100			
[COM005] Fibra	B	1	100			
[MEDIA001] Discos duros extraíbles	B	10	10			
[MEDIA002] Blue-Ray	B	10	100			
[L001] Nave principal	B	10	100			
[L005] CPD	M	10	100			

Tabla 48. Ficha de amenazas [A.12] Análisis de trafico

[A.12] Análisis de trafico						
Tipos de activos afectados: [COM]		**Dimensiones a las que afecta:** [C]				
Descripción: el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[COM001] Red local LAN	MB		100			
[COM005] Fibra	MB		100			

Tabla 49. Ficha de amenazas [A.13] Repudio

[A.13] Repudio						
Tipos de activos afectados: [D.LOG], [S]		**Dimensiones a las que afecta:** [I]				
Descripción: negación a posteriori de actuaciones o compromisos adquiridos en el pasado.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D006] Ficheros LOG	B	10				100
[S003] VPN	MB	10				100
[S004] Virtualización servidores	B	10				100
[S007] DNS	MB	10				100
[S009] Active directory	MB	10				100
[S010] GPO	MB	10				10
[S015] Servidor ERP	MB	10				10
[S016] PostgreSQL	B	10				10
[S017] Microsoft SQLServer	B	10				10

Tabla 50. Ficha de amenazas [A.14] Interceptación de información (escucha)

[A.14] Interceptación de información (escucha)						
Tipos de activos afectados: [COM]		**Dimensiones a las que afecta:** [C]				
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[COM001] Red local LAN	MB		100			
[COM005] Fibra	MB		100			

Tabla 51. Ficha de amenazas [A.15] Modificación deliberada de la información

[A.15] Modificación deliberada de la información						
Tipos de activos afectados: [D], [KEYS], [S], [SW], [COM], [MEDIA], [L]		**Dimensiones a las que afecta:** [I]				
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D001] Documentación y planos de la producción	M	100				
[D002] Archivo clientes	M	100				
[D005] Copias de seguridad	MB	100				
[D006] Ficheros log	MB	100				
[D007] Ficheros configuración	MB	100				
[D008] Base de datos del ERP	MB	100				
[D009] BD del Gestor de proyectos	MB	100				
[D010] Datos personal empresa	B	100				
[S003] VPN	MB	10				
[S004] Virtualización servidores	MB	10				

[S007] DNS	MB	10				
[S009] Active directory	MB	100				
[S010] GPO	MB	10				
[S015] Servidor ERP	MB	100				
[S016] PostgreSQL	MB	100				
[S017] Microsoft SQLServer	MB	100				
[SW002] Cliente de correo	MB	100				
[SW005] ERP (Microsoft Dynamics Navision 2017)	M	100				
[SW006] Suite de diseño grafico	MB	100				
[SW007] Antivirus	MB	100				
[SW008] Sistema operativo	MB	10				
[SW009] Sistema de backup	MB	100				
[SW011] Software de fabricación	M	10				
[SW012] Software de gestión de proyectos	M	100				
[COM001] Red local LAN	B	10				
[COM005] Fibra	B	10				
[MEDIA001] Discos duros extraíbles	MB	100				
[MEDIA002] Blue-Ray	MB	100				
[L001] Nave principal	MB	100				
[L005] CPD	MB	10				

Tabla 52. Ficha de amenazas [A.18] Destrucción de la información

[A.18] Destrucción de la información						
Tipos de activos afectados: [D], [KEYS], [S], [SW], [MEDIA], [L]		**Dimensiones a las que afecta:** [D], [I]				
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D001] Documentación y planos de la producción	B			100		
[D002] Archivo clientes	MB			100		
[D005] Copias de seguridad	MB			100		
[D006] Ficheros log	MB			100		
[D007] Ficheros configuración	MB			100		
[D008] Base de datos del ERP	MB			100		
[D009] BD del Gestor de proyectos	MB			100		
[D010] Datos personal empresa	MB			100		
[S003] VPN	MB			10		
[S004] Virtualización servidores	MB			10		
[S007] DNS	MB			100		
[S009] Active directory	MB			100		
[S010] GPO	MB			100		
[S015] Servidor ERP	MB			100		
[S016] PostgreSQL	MB			100		
[S017] Microsoft SQLServer	MB			100		
[SW002] Cliente de correo	MB			100		
[SW005] ERP (Microsoft Dynamics Navision 2017)	MB			10		
[SW006] Suite de diseño grafico	MB			100		
[SW007] Antivirus	MB			10		

[SW008] Sistema operativo	MB			100		
[SW009] Sistema de backup	MB			100		
[SW011] Software de fabricación	B			100		
[SW012] Software de gestión de proyectos	B			100		
[MEDIA001] Discos duros extraíbles	MB			100		
[MEDIA002] Blue-Ray	MB			100		
[L001] Nave principal	MB			100		
[L005] CPD	MB			100		

Tabla 53. Ficha de amenazas [A.19] Divulgación de información

[A.19] Divulgación de información						
Tipos de activos afectados: [D], [KEYS], [S], [SW], [COM], [MEDIA], [L]		**Dimensiones a las que afecta:** [C]				
Descripción: revelación intencionada de información.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[D001] Documentación y planos de la producción	B		100			
[D002] Archivo clientes	B		100			
[D005] Copias de seguridad	MB		100			
[D006] Ficheros log	MB		100			
[D007] Ficheros configuración	MB		100			
[D008] Base de datos del ERP	MB		100			
[D009] BD del Gestor de proyectos	MB		100			
[D010] Datos personal empresa	B		100			
[S003] VPN	MB		100			
[S004] Virtualización servidores	MB		100			
[S007] DNS	MB		100			
[S009] Active directory	MB		100			

[S010] GPO	MB		100			
[S015] Servidor ERP	MB		100			
[S016] PostgreSQL	MB		100			
[S017] Microsoft SQLServer	MB		100			
[SW002] Cliente de correo	B		100			
[SW005] ERP (Microsoft Dynamics Navision 2017)	B		100			
[SW006] Suite de diseño grafico	MB		100			
[SW007] Antivirus	MB		1			
[SW008] Sistema operativo	MB		100			
[SW009] Sistema de backup	MB		100			
[SW011] Software de fabricación	B		100			
[SW012] Software de gestión de proyectos	B		100			
[COM001] Red local LAN	M		10			
[COM005] Fibra	M		10			
[MEDIA001] Discos duros extraíbles	MB		10			
[MEDIA002] Blue-Ray	MB		100			
[L001] Nave principal	MB		100			
[L005] CPD	MB		100			

Tabla 54. Ficha de amenazas [A.22] Manipulación de los programas (software)

[A.22] Manipulación de los programas (software)						
Tipos de activos afectados: [SW]		**Dimensiones a las que afecta:** [C], [I], [D]				
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[SW002] Cliente de correo	MB	10	100	10		

[SW005] ERP (Microsoft Dynamics Navision 2017)	MB	10	100	10		
[SW006] Suite de diseño grafico	MB	10	100	10		
[SW007] Antivirus	MB	1	1	1		
[SW008] Sistema operativo	MB	1	1	1		
[SW009] Sistema de backup	MB	10	10	10		
[SW011] Software de fabricación	MB	10	100	10		
[SW012] Software de gestión de proyectos	MB	10	100	10		

Tabla 55. Ficha de amenazas [A.23] Manipulación de los equipos

[A.23] Manipulación de los equipos						
Tipos de activos afectados: [HW], [MEDIA], [AUX]		**Dimensiones a las que afecta:** [C], [D]				
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	MB		10	10		
[HW006] NAS (2)	MB		10	10		
[HW007] Router	MB		100	100		
[HW009] Servidores físicos (3)	MB		10	10		
[HW010] Servidores virtualizados (12)	MB		10	10		
[HW011] Switch (12)	MB		100	10		
[HW014] Mini-switch (15)	MB		100	10		
[HW016] Terminales (20)	MB		10	10		
[HW018] Servidor de copias	MB		10	10		
[MEDIA001] Discos duros extraíbles	MB		1	1		
[MEDIA002] Blue-Ray	MB		1	1		

Tabla 56. Ficha de amenazas [A.24] Denegación de servicio

[A.24] Denegación de servicio						
Tipos de activos afectados: [S], [HW], [COM]		**Dimensiones a las que afecta:** [D]				
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[S003] VPN	MB			100		
[S004] Virtualización servidores	MB			100		
[S007] DNS	MB			100		
[S009] Active directory	MB			100		
[S010] GPO	MB			100		
[S015] Servidor ERP	MB			100		
[S016] PostgreSQL	MB			100		
[S017] Microsoft SQLServer	MB			100		
[HW003] Ordenadores diseño (15)	MB			100		
[HW006] NAS (2)	MB			100		
[HW007] Router	M			100		
[HW009] Servidores físicos (3)	MB			100		
[HW010] Servidores virtualizados (12)	MB			100		
[HW011] Switch (12)	MB			100		
[HW014] Mini-switch (15)	B			100		
[HW016] Terminales (20)	MB			100		
[HW018] Servidor de copias	MB			100		
[COM001] Red local LAN	B			100		
[COM005] Fibra	M			100		

Tabla 57. Ficha de amenazas [A.25] Robo

[A.25] Robo						
Tipos de activos afectados: [HW], [MEDIA], [AUX]		**Dimensiones a las que afecta:** [D], [C]				
Descripción: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	B		100	100		
[HW006] NAS (2)	B		100	100		
[HW007] Router	B		10	100		
[HW009] Servidores físicos (3)	B		100	100		
[HW010] Servidores virtualizados (12)	B		1	100		
[HW011] Switch (12)	B		1	100		
[HW014] Mini-switch (15)	B		1	100		
[HW016] Terminales (20)	MB		100	100		
[HW018] Servidor de copias	B		100	100		
[MEDIA001] Discos duros extraíbles	B		100	100		
[MEDIA002] Blue-Ray	B		100	100		

Tabla 58. Ficha de amenazas [A.26] Ataque destructivo

[A.26] Ataque destructivo						
Tipos de activos afectados: [HW], [MEDIA], [AUX], [L]		**Dimensiones a las que afecta:** [D]				
Descripción: vandalismo, terrorismo, acción militar, ...						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[HW003] Ordenadores diseño (15)	MB			100		

[HW006] NAS (2)	MB			100		
[HW007] Router	MB			100		
[HW009] Servidores físicos (3)	MB			100		
[HW010] Servidores virtualizados (12)	MB			100		
[HW011] Switch (12)	MB			100		
[HW014] Mini-switch (15)	MB			100		
[HW016] Terminales (20)	MB			100		
[HW018] Servidor de copias	MB			100		
[MEDIA001] Discos duros extraíbles	MB			100		
[MEDIA002] Blue-Ray	MB			100		
[L001] Nave principal	MB			100		
[L005] CPD	MB			100		

Tabla 59. Ficha de amenazas [A.27] Ocupación enemiga

[A.27] Ocupación enemiga						
Tipos de activos afectados: [L]		**Dimensiones a las que afecta:** [D], [C]				
Descripción: cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[L001] Nave principal	MB		100	100		
[L005] CPD	MB		100	100		

Tabla 60. Ficha de amenazas [A.28] Indisponibilidad del personal

[A.28] Indisponibilidad del personal						
Tipos de activos afectados: [P]		**Dimensiones a las que afecta:** [D]				
Descripción: ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral…						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[P001] Gerencia	B			100		
[P002] Oficina	B			10		

Tabla 61. Ficha de amenazas [A.29] Extorsión

[A.29] Extorsión						
Tipos de activos afectados: [P]		**Dimensiones a las que afecta:** [C], [I], [D]				
Descripción: presión que se ejerce sobre alguien para obligarle a obrar en determinado sentido.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[P001] Gerencia	MB	100	100	100		
[P002] Oficina	MB	10	100	10		

Tabla 62. Ficha de amenazas [A.30] Ingeniería social (picaresca)

[A.30] Ingeniería social (picaresca)						
Tipos de activos afectados: [P]		**Dimensiones a las que afecta:** [C], [I], [D]				
Descripción: abuso de la buena fe de la gente para que realicen actividades maliciosas.						
Activos afectados	**Probabilidad**	**% Degradación**				
		[I]	**[C]**	**[D]**	**[A]**	**[T]**
[P001] Gerencia	B	100	100	100		
[P002] Oficina	B	10	100	100		

7.3. Cálculo del impacto y riesgo

Ahora que ya se ha conseguido recopilar el catálogo de activos y las amenazas que pueden manifestarse sobre estos, se puede averiguar cómo afectan las amenazas y los riesgos que conlleva. Para ello, el siguiente paso es determinar cuál es el impacto que causan estás amenazas sobre cada uno de los activos para posteriormente determinar el riesgo.

Se denomina impacto al daño causado por la materialización de una amenaza sobre un activo. Para calcular el impacto de una amenaza sobre un activo en concreto, utilizaremos el método de análisis mediante tablas, incluido en el libro 3, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, de la metodología Magerit v3 [11].

Para cada amenaza que puede actuar sobre cada dimensión de un activo, se ha de calcular el grado de degradación sobre esa dimensión, a mayor degradación sobre una dimensión de mayor valor, el impacto será mayor.

Tabla 63. Calculo de Impacto (Fuente MAGERIT v3 Libro III [11])

Impacto		**Degradación**		
		1%	10%	100%
Valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Una vez que se tiene el impacto, se ha de calcular la probabilidad de ocurrencia de una amenaza, siendo el cruce entre impacto y probabilidad lo nos proporcionará el riesgo de una amenaza sobre un activo.

Tabla 64. Matriz estimación del riesgo (impacto vs probabilidad). (Fuente MAGERIT v3 Libro III [11])

Riesgo		**Probabilidad**				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Además, definimos las escalas que emplearemos para asignar valores nominales a los posibles valores asignables al impacto, la probabilidad y el riesgo.

Tabla 65. Escalas cualitativas para el modelado de impacto, probabilidad y riesgo

Escalas		
Impacto	**Probabilidad**	**Riesgo**
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB**: muy bajo	**MB**: despreciable

Los valores MA de riesgo e impacto serán aquellos que requerirán una atención inmediata, adquiriendo el foco de atención para los futuros planes de seguridad.

A continuación, detallamos las fichas para cada activo de los que hemos seleccionado con la información de las amenazas que puedan sufrir, además del impacto y el riesgo potencial.

Para ello contamos con el siguiente modelo de ficha, esta se encuentra detallada por dimensiones de valoración.

Tabla 66. Ejemplo ficha de cálculo impacto/riesgo por activo (Elaboración propia)

[D] Datos / Información		**D001 - Documentación y datos**														
Valor		**[I]**		**[C]**		**[D]**		**[A]**		**[T]**		**TOTAL**				
		A		A		MA		MA		MA		MA				
Amenazas	**Probabilidad**	**Degradación**					**Impacto potencial**					**Riesgo potencial**				
	Frecuencia	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**
[E.1] Errores de los usuarios	A	10	10	10			M	M	A			A	A	MA		

7.3.1. [D] Datos / Información (impacto y riesgo potencial)

Tabla 67. Impacto y Riesgo (potencial) del activo D001-Documentación y datos

[D] Datos / Información		D001 - Documentación y datos														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		A		MA		MA		MA		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	A	10	10	10			M	M	A			A	A	MA		
[E.2] Errores del administrador	MB	10	10	10			M	M	A			B	B	M		
[E.15] Alteración accidental de la información	M	10					M					M				
[E.18] Destrucción de la información	M			100					MA					MA		
[E.19] Fugas de información	B		100					A					A			
[A.5] Suplantación de la identidad del usuario	B	10	100		10		M	A		A		M	A		A	
[A.6] Abuso de privilegios de acceso	A	10	100	10			M	A	A			A	MA	MA		
[A.11] Acceso no autorizado	B	10	100				M	A				M	A			
[A.15] Modificación deliberada de la información	M	100					A					A				
[A.18] Destrucción de la información	B			100					MA					MA		
[A.19] Divulgación de información	B		100					A					A			

Tabla 68. Impacto y Riesgo (potencial) del activo D002-Archivo clientes

[D] Datos / Información		D002 – Archivo clientes														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA		MA		MA		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	M	10	10	1			A	A	M			A	A	M		
[E.2] Errores del administrador	MB	10	10	10			A	A	A			M	M	M		
[E.15] Alteración accidental de la información	M	10					A					A				
[E.18] Destrucción de la información	B			100					MA					MA		
[E.19] Fugas de información	MB		10					A					M			
[A.5] Suplantación de la identidad del usuario	B	10	100		10		A	MA		A		A	MA		A	
[A.6] Abuso de privilegios de acceso	M	10	100	10			A	MA	A			A	MA	A		
[A.11] Acceso no autorizado	B	10	100				A	MA				A	MA			
[A.15] Modificación deliberada de la información	M	100					MA					MA				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	B		100					MA					MA			

Tabla 69. Impacto y Riesgo (potencial) del activo D005-Copias de seguridad

[D] Datos / Información		D005 – Copias de seguridad														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		A		A		A		M		A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			B	B	B			MB	MB	MB		
[E.2] Errores del administrador	M	100	10	10			A	M	M			A	M	M		
[E.15] Alteración accidental de la información	MB	1					B					MB				
[E.18] Destrucción de la información	MB			100					A					M		
[E.19] Fugas de información	MB		1					B					MB			
[A.5] Suplantación de la identidad del usuario	MB	10	100		10		M	A		M		B	M		B	
[A.6] Abuso de privilegios de acceso	MB	10	10	10			M	M	M			B	B	B		
[A.11] Acceso no autorizado	MB	10	100				M	A				B	M			
[A.15] Modificación deliberada de la información	MB	100					A					M				
[A.18] Destrucción de la información	MB			100					A					M		
[A.19] Divulgación de información	MB		100					A					M			

Tabla 70. Impacto y Riesgo (potencial) del activo D006-Ficheros de LOG

[D] Datos / Información		D006 – Ficheros de LOG														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		M		A		M		M		A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			MB	MB	B			MB	MB	MB		
[E.2] Errores del administrador	MB	10	10	10			B	B	M			MB	MB	B		
[E.15] Alteración accidental de la información	MB	1					MB					MB				
[E.18] Destrucción de la información	B			10					M					M		
[E.19] Fugas de información	MB		1					MB					MB			
[A.5] Suplantación de la identidad del usuario	MB	10	100		10		B	M		B		MB	B		MB	
[A.6] Abuso de privilegios de acceso	MB	10	10	10			B	B	M			MB	MB	B		
[A.11] Acceso no autorizado	MB	10	100				B	M				MB	B			
[A.15] Modificación deliberada de la información	MB	100					M					B				
[A.18] Destrucción de la información	MB			100					A					M		
[A.19] Divulgación de información	MB		100					M					B			

Tabla 71. Impacto y Riesgo (potencial) del activo D007-Ficheros de configuración

[D] Datos / Información		D007 – Ficheros configuración														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		A		MA		A		MA		A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	B	M			B	MB	B		
[E.2] Errores del administrador	M	10	10	10			A	M	A			A	M	A		
[E.15] Alteración accidental de la información	B	10					A					A				
[E.18] Destrucción de la información	B			100					MA					MA		
[E.19] Fugas de información	MB		10					M					B			
[A.5] Suplantación de la identidad del usuario	MB	10	100		10		A	A		M		M	M		B	
[A.6] Abuso de privilegios de acceso	MB	10	10	10			A	M	A			M	B	M		
[A.11] Acceso no autorizado	MB	10	100				A	A				M	M			
[A.15] Modificación deliberada de la información	MB	100					MA					A				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					A					M			

Tabla 72. Impacto y Riesgo (potencial) del activo D008-Base de datos del ERP

[D] Datos / Información		D008 – Base de datos del ERP														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA		MA		MA		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	M	M			B	B	B		
[E.2] Errores del administrador	M	10	10	10			A	A	A			A	A	A		
[E.15] Alteración accidental de la información	MB	1					M					B				
[E.18] Destrucción de la información	B			100					MA					MA		
[E.19] Fugas de información	MB		1					M					B			
[A.5] Suplantación de la identidad del usuario	MB	10	100		10		A	MA		A		M	A		M	
[A.6] Abuso de privilegios de acceso	MB	10	10	10			A	A	A			M	M	M		
[A.11] Acceso no autorizado	MB	10	100				A	MA				M	A			
[A.15] Modificación deliberada de la información	MB	100					MA					A				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					MA					A			

Tabla 73. Impacto y Riesgo (potencial) del activo D009-BD del gestor de proyectos

[D] Datos / Información		D009 - BD del Gestor de proyectos														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		A		MA		MA		A		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	B	M			B	MB	B		
[E.2] Errores del administrador	M	100	10	10			MA	M	A			MA	M	A		
[E.15] Alteración accidental de la información	B	1					M					M				
[E.18] Destrucción de la información	B			100					MA					MA		
[E.19] Fugas de información	MB		1					B					MB			
[A.5] Suplantación de la identidad del usuario	MB	10	100		10		A	A		A		M	M		M	
[A.6] Abuso de privilegios de acceso	MB	10	10	10			A	M	A			M	B	M		
[A.11] Acceso no autorizado	MB	10	100				A	A				M	M			
[A.15] Modificación deliberada de la información	MB	100					MA					A				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					A					M			

Tabla 74. Impacto y Riesgo (potencial) del activo D010-Datos personal empresa

[D] Datos / Información		D010 – Datos personal empresa														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		MA		A		MA		MA		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	M	10	10	1			M	A	B			M	A	B		
[E.2] Errores del administrador	MB	10	10	10			M	A	M			B	M	B		
[E.15] Alteración accidental de la información	M	10					M					M				
[E.18] Destrucción de la información	B			100					A					A		
[E.19] Fugas de información	B		10					A					A			
[A.5] Suplantación de la identidad del usuario	B	10	100		10		M	MA		A		M	MA		A	
[A.6] Abuso de privilegios de acceso	M	10	100	10			M	MA	M			M	MA	M		
[A.11] Acceso no autorizado	B	10	100				M	MA				M	MA			
[A.15] Modificación deliberada de la información	B	100					A					A				
[A.18] Destrucción de la información	MB			100					A					M		
[A.19] Divulgación de información	B		100					MA					MA			

7.3.2. [S] Servicios (impacto y riesgo potencial)

Tabla 75. Impacto y Riesgo (potencial) del activo S003-VPN

[S] Servicios		S003 - VPN														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		MA		M		A		A		A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			B	M	MB			MB	B	MB		
[E.2] Errores del administrador	B	1	1	10			B	M	M			B	M	M		
[E.9] Errores de re-encaminamiento	MB		100					MA					A			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental	MB	10					M					B				
[E.18] Destrucción de la información	MB			1					MB					MB		
[E.19] Fugas de información	MB		1					M					B			
[E.24] Caída del sistema por agotamiento de recursos	B			10					M					M		
[A.5] Suplantación identidad	B	1	10		100		B	A		A		B	A		A	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			B	M	MB			MB	B	MB		
[A.7] Uso no previsto	MB	10	10	10			M	A	M			B	M	B		
[A.9] Re-encaminamiento mensajes	MB		100					MA					A			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	MB	1	100				B	MA				B	A			
[A.13] Repudio	MB	10				100	M				M	B				B
[A.15] Modificación deliberada	MB	10					M					B				
[A.18] Destrucción de la información	MB			10					M					B		
[A.19] Divulgación de información	MB		100					MA					A			
[A.24] Denegación de servicio	MB			100					M					B		

Tabla 76. Impacto y Riesgo (potencial) del activo S004-Virtualizacion servidores

[S] Servicios		S004 – Virtualización servidores														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		M		A		M		A		A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			MB	MB	B			MB	MB	MB		
[E.2] Errores del administrador	B	10	1	10			B	MB	M			B	MB	M		
[E.9] Errores de re-encaminamiento	MB		1					MB					MB			
[E.10] Errores de secuencia	MB	1					MB					MB				
[E.15] Alteración accidental de la información	MB	10					B					MB				
[E.18] Destrucción de la información	MB			1					B					MB		
[E.19] Fugas de información	MB		1					MB					MB			
[E.24] Caída del sistema por agotamiento de recursos	B			10					M					M		
[A.5] Suplantación de la identidad	MB	1	100		10		MB	M		B		MB	B		MB	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			MB	MB	B			MB	MB	MB		
[A.7] Uso no previsto	MB	10	10	10			B	B	M			MB	MB	B		
[A.9] [Re-]encaminamiento de mensajes	MB		10					B					MB			
[A.10] Alteración de secuencia	MB	1					MB					MB				
[A.11] Acceso no autorizado	MB	10	100				B	M				MB	B			
[A.13] Repudio	B	10				100	B				A	B				A
[A.15] Modificación deliberada	MB	10					B					MB				
[A.18] Destrucción de la información	MB			10					M					B		
[A.19] Divulgación de información	MB		100					M					B			
[A.24] Denegación de servicio	MB			100					A					M		

Tabla 77. Impacto y Riesgo (potencial) del activo S007-DNS

[S] Servicios		S007 - DNS														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		MB		MA		A		B		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			B	MB	M			MB	MB	B		
[E.2] Errores del administrador	B	1	1	10			B	MB	A			B	MB	A		
[E.9] Errores de re-encaminamiento	MB		100					MB					MB			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental de la información	MB	1					B					MB				
[E.18] Destrucción de la información	MB			1					M					B		
[E.19] Fugas de información	MB		1					MB					MB			
[E.24] Caída del sistema por agotamiento de recursos	MB			1					M					B		
[A.5] Suplantación de la identidad del usuario	MB	1	100		100		B	MB		A		MB	MB		M	
[A.6] Abuso de privilegios de acceso	MB	1	1	10			B	MB	A			MB	MB	M		
[A.7] Uso no previsto	MB	10	10	10			M	MB	A			B	MB	M		
[A.9] [Re-]encaminamiento de mensajes	MB		100					MB					MB			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	MB	10	100				M	MB				B	MB			
[A.13] Repudio	MB	10				100	M				B	B				MB
[A.15] Modificación deliberada de la información	MB	10					M					B				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					MB					MB			
[A.24] Denegación de servicio	MB			100					MA					A		

Tabla 78. Impacto y Riesgo (potencial) del activo S009-Active Directory

[S] Servicios		S009 – Active Directory														
Valor		[I]		[C]		[D]	[A]			[T]	TOTAL					
		M		A		MA	M			A	MA					
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			MB	B	M			MB	MB	B		
[E.2] Errores del administrador	B	10	1	1			B	B	M			B	B	M		
[E.9] Errores de re-encaminamiento	MB		10					M					MB			
[E.10] Errores de secuencia	MB	1					MB					MB				
[E.15] Alteración accidental de la información	MB	1					MB					MB				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	MB		1					B					MB			
[E.24] Caída del sistema por agotamiento de recursos	MB			1					M					B		
[A.5] Suplantación de la identidad del usuario	MB	1	100		100		MB	A		M		MB	M		B	
[A.6] Abuso de privilegios de acceso	MB	1	10	10			MB	M	A			MB	B	M		
[A.7] Uso no previsto	MB	10	10	10			B	M	A			MB	B	M		
[A.9] [Re-]encaminamiento de mensajes	MB		10					M					B			
[A.10] Alteración de secuencia	MB	1					MB					MB				
[A.11] Acceso no autorizado	MB	10	100				B	A				MB	M			
[A.13] Repudio	MB	10				100	B				A	MB				M
[A.15] Modificación deliberada de la información	MB	100					M					B				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					A					M			
[A.24] Denegación de servicio	MB			100					MA					A		

Tabla 79. Impacto y Riesgo (potencial) del activo S010-GPO

[S] Servicios		S010 - GPO														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		M		MA		B		A		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			B	MB	M			MB	MB	B		
[E.2] Errores del administrador	B	1	1	10			B	MB	A			B	MB	A		
[E.9] Errores de re-encaminamiento	MB		10					B					MB			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental de la información	MB	1					B					MB				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	MB		1					MB					MB			
[E.24] Caída del sistema por agotamiento de recursos	MB			1					M					B		
[A.5] Suplantación de la identidad del usuario	MB	1	10		100		B	B		B		MB	MB		MB	
[A.6] Abuso de privilegios de acceso	MB	1	10	10			B	B	A			MB	MB	M		
[A.7] Uso no previsto	MB	10	10	10			M	B	A			B	MB	M		
[A.9] [Re-]encaminamiento de mensajes	MB		10					B					MB			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	MB	10	100				M	M				B	B			
[A.13] Repudio	MB	10				10	M				M	B				B
[A.15] Modificación deliberada de la información	MB	10					M					B				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					M					B			
[A.24] Denegación de servicio	MB			100					MA					A		

Tabla 80. Impacto y Riesgo (potencial) del activo S015-Servidor ERP

[S] Servicios		S015 – Servidor ERP														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		A		MA		MA		MA		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	B	M			B	MB	B		
[E.2] Errores del administrador	M	1	1	10			M	B	A			M	B	A		
[E.9] Errores de re-encaminamiento	MB		100					A					M			
[E.10] Errores de secuencia	MB	1					M					B				
[E.15] Alteración accidental	MB	10					A					M				
[E.18] Destrucción de la información	MB			1					M					B		
[E.19] Fugas de información	MB		1					B					MB			
[E.24] Caída del sistema por agotamiento de recursos	B			1					M					M		
[A.5] Suplantación de la identidad del usuario	MB	1	10		100		M	M		MA		B	B		A	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			M	B	M			B	MB	B		
[A.7] Uso no previsto	MB	10	10	10			A	M	A			M	B	M		
[A.9] [Re-]encaminamiento de mensajes	MB		10					M					B			
[A.10] Alteración de secuencia	MB	1					M					B				
[A.11] Acceso no autorizado	MB	10	100				A	A				M	M			
[A.13] Repudio	MB	10				10	A				A	M				M
[A.15] Modificación deliberada	MB	100					MA					A				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					A					M			
[A.24] Denegación de servicio	MB			100					MA					A		

Tabla 81. Impacto y Riesgo (potencial) del activo S016- PostgreSQL

[S] Servicios		S016 - PostgreSQL														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		A		MA		MA		MA		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	B	M			B	MB	B		
[E.2] Errores del administrador	B	1	1	10			M	B	A			M	B	A		
[E.9] Errores de re-encaminamiento	MB		100					A					M			
[E.10] Errores de secuencia	MB	1					M					B				
[E.15] Alteración accidental de la información	M	10					A					A				
[E.18] Destrucción de la información	B			100					MA					MA		
[E.19] Fugas de información	MB		1					B					MB			
[E.24] Caída del sistema por agotamiento de recursos	B			10					A					A		
[A.5] Suplantación de la identidad del usuario	MB	1	100		100		M	A		MA		B	M		A	
[A.6] Abuso de privilegios de acceso	MB	1	10	10			M	M	A			B	B	M		
[A.7] Uso no previsto	MB	10	10	10			A	M	A			M	B	M		
[A.9] [Re-]encaminamiento de mensajes	MB		100					A					M			
[A.10] Alteración de secuencia	MB	1					M					B				
[A.11] Acceso no autorizado	B	10	100				A	A				A	A			
[A.13] Repudio	B	10				10	A				A	A				A
[A.15] Modificación deliberada de la información	MB	100					MA					A				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					A					M			
[A.24] Denegación de servicio	MB			100					MA					A		

Tabla 82. Impacto y Riesgo (potencial) del activo S017- Microsoft SQLServer

[S] Servicios		S017 - Microsoft SQLServer														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		A		MA		MA		MA		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	B	M			B	MB	B		
[E.2] Errores del administrador	B	1	1	10			M	B	A			M	B	A		
[E.9] Errores de re-encaminamiento	MB		100					A					M			
[E.10] Errores de secuencia	MB	1					M					B				
[E.15] Alteración accidental de la información	M	10					A					A				
[E.18] Destrucción de la información	B			100					MA					MA		
[E.19] Fugas de información	MB		1					B					MB			
[E.24] Caída del sistema por agotamiento de recursos	B			10					A					A		
[A.5] Suplantación de la identidad del usuario	MB	1	100		100		M	A		MA		B	M		A	
[A.6] Abuso de privilegios de acceso	MB	1	10	10			M	M	A			B	B	M		
[A.7] Uso no previsto	MB	10	10	10			A	M	A			M	B	M		
[A.9] [Re-]encaminamiento de mensajes	MB		100					A					M			
[A.10] Alteración de secuencia	MB	1					M					B				
[A.11] Acceso no autorizado	B	10	100				A	A				A	A			
[A.13] Repudio	B	10				10	A				A	A				A
[A.15] Modificación deliberada de la información	MB	100					MA					A				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					A					M			
[A.24] Denegación de servicio	MB			100					MA					A		

7.3.3. [SW] Software (impacto y riesgo potencial)

Tabla 83. Impacto y Riesgo (potencial) del activo SW002- Cliente de correo

[SW] Software		SW002 - Cliente de correo														
Valor		[I]	[C]	[D]	[A]	[T]	[A]					TOTAL				
		A	MA	MA	MA	A						A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	MB			10					A					M		
[E.1] Errores de los usuarios	B	1	1	10			B	M	A			B	M	A		
[E.2] Errores del administrador	B	1	1	10			B	M	A			B	M	A		
[E.8] Difusión de software dañino	B	10	100	10			M	MA	A			M	MA	A		
[E.9] Errores de re-encaminamiento	MB		10					A					M			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental de la información	B	1					B					B				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	M		100					MA					MA			
[E.20] Vulnerabilidades de los programas (software)	MB	10	100	10			M	MA	A			B	A	M		
[E.21] Errores de mantenimiento / actualización de programas	MB	10	10	10			M	A	A			B	M	M		
[A.5] Suplantación de la identidad del usuario	MB	10	100		100		M	MA		MA		B	A		A	
[A.6] Abuso de privilegios de acceso	MB	10	10	1			M	A	M			B	M	B		
[A.7] Uso no previsto	B	10	100	10			M	MA	A			M	MA	A		
[A.8] Difusión de software dañino	MB	10	100	10			M	MA	A			B	A	M		
[A.9] [Re-]encaminamiento de mensajes	MB		10					A					M			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	MB	10	100				M	MA				B	A			
[A.15] Modificación deliberada de la información	MB	100					A					A				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	B		100					MA					MA			
[A.22] Manipulación de los programas	MB	10	100	10			M	MA	A			B	A	M		

Tabla 84. Impacto y Riesgo (potencial) del activo SW005- ERP

[SW] Software		SW005 - ERP														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA		MA		MA		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	B			10					A					A		
[E.1] Errores de los usuarios	MA	10	100	1			A	MA	M			MA	MA	A		
[E.2] Errores del administrador	B	1	10	10			M	A	A			M	A	A		
[E.8] Difusión de software dañino	MB	100	100	100			MA	MA	MA			A	A	A		
[E.9] Errores de re-encaminamiento	MB		10					A					M			
[E.10] Errores de secuencia	MB	1					M					B				
[E.15] Alteración accidental de la información	B	10					A					A				
[E.18] Destrucción de la información	MB			100					MA					A		
[E.19] Fugas de información	MB		100					MA					A			
[E.20] Vulnerabilidades de los programas (software)	B	10	100	10			A	MA	A			A	MA	A		
[E.21] Errores de mantenimiento / actualización de programas	B	10	10	10			A	A	A			A	A	A		
[A.5] Suplantación de la identidad del usuario	MB	10	100		100		A	MA		MA		M	A		A	
[A.6] Abuso de privilegios de acceso	A	10	100	10			A	MA	A			MA	MA	MA		
[A.7] Uso no previsto	B	10	10	10			A	A	A			A	A	A		
[A.8] Difusión de software dañino	MB	100	100	100			MA	MA	MA			A	A	A		
[A.9] [Re-]encaminamiento de mensajes	MB		1					M					B			
[A.10] Alteración de secuencia	MB	1					M					B				
[A.11] Acceso no autorizado	B	10	100				A	MA				A	MA			
[A.15] Modificación deliberada de la información	M	100					MA					MA				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	B		100					MA					MA			
[A.22] Manipulación de los programas	MB	10	100	10			A	MA	A			M	A	M		

Tabla 85. Impacto y Riesgo (potencial) del activo SW006- Suite de diseño grafico

[SW] Software		SW006 - Suite de diseño grafico														
Valor		[I]	[C]	[D]	[A]	[T]	[A]					TOTAL				
		M	A	A	M	A						A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	B			10					M					M		
[E.1] Errores de los usuarios	M	10	10	10			B	M	M			B	M	M		
[E.2] Errores del administrador	MB	1	1	1			MB	B	B			MB	MB	MB		
[E.8] Difusión de software dañino	MB	10	1	10			B	B	M			MB	MB	B		
[E.9] Errores de re-encaminamiento	MB		1					B					MB			
[E.10] Errores de secuencia	MB	1					MB					MB				
[E.15] Alteración accidental de la información	MB	10					B					MB				
[E.18] Destrucción de la información	MB			10					M					B		
[E.19] Fugas de información	MB		1					B					MB			
[E.20] Vulnerabilidades de los programas (software)	B	10	10	10			B	M	M			B	M	M		
[E.21] Errores de mantenimiento / actualización de programas	B	10	1	10			B	B	M			B	B	M		
[A.5] Suplantación de la identidad del usuario	MB	1	10		100		MB	M		M		MB	B		B	
[A.6] Abuso de privilegios de acceso	MB	10	10	10			B	M	M			MB	B	B		
[A.7] Uso no previsto	B	10	10	100			B	M	A			B	M	A		
[A.8] Difusión de software dañino	MB	10	1	10			B	B	M			MB	MB	B		
[A.9] [Re-]encaminamiento de mensajes	MB		1					B					MB			
[A.10] Alteración de secuencia	MB	1					MB					MB				
[A.11] Acceso no autorizado	MB	10	10				B	M				MB	B			
[A.15] Modificación deliberada de la información	MB	100					M					B				
[A.18] Destrucción de la información	MB			100					A					M		
[A.19] Divulgación de información	MB		100					A					M			
[A.22] Manipulación de los programas	MB	10	100	10			B	A	M			MB	M	B		

Tabla 86. Impacto y Riesgo (potencial) del activo SW007- Antivirus

[SW] Software		SW007 - Antivirus														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		B		MA		M		M		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	MB			10					A					M		
[E.1] Errores de los usuarios	MB	1	1	1			M	MB	M			B	MB	B		
[E.2] Errores del administrador	MB	1	1	1			M	MB	M			B	MB	B		
[E.8] Difusión de software dañino	MB	10	1	10			A	MB	A			M	MB	M		
[E.9] Errores de re-encaminamiento	MB		1					MB					MB			
[E.10] Errores de secuencia	MB	1					M					B				
[E.15] Alteración accidental de la información	MB	1					M					B				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	MB		1					MB					MB			
[E.20] Vulnerabilidades de los programas (software)	MB	100	10	10			MA	MB	A			A	MB	M		
[E.21] Errores de mantenimiento / actualización de programas	MB	100	1	10			MA	MB	A			A	MB	M		
[A.5] Suplantación de la identidad del usuario	MB	10	10		100		A	MB		M		M	MB		B	
[A.6] Abuso de privilegios de acceso	MB	100	10	10			MA	MB	A			A	MB	M		
[A.7] Uso no previsto	MB	10	10	10			A	MB	A			M	MB	M		
[A.8] Difusión de software dañino	MB	10	1	10			A	MB	A			M	MB	M		
[A.9] [Re-]encaminamiento de mensajes	MB		1					MB					MB			
[A.10] Alteración de secuencia	MB	1					M					B				
[A.11] Acceso no autorizado	MB	100	10				MA	MB				A	MB			
[A.15] Modificación deliberada de la información	MB	100					MA					A				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		1					MB					MB			
[A.22] Manipulación de los programas	MB	1	1	1			M	MB	M			B	MB	B		

Tabla 87. Impacto y Riesgo (potencial) del activo SW008- Sistema operativo

[SW] Software		SW008 - Sistema operativo														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		A		MA		M		A		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	B			10					A					A		
[E.1] Errores de los usuarios	B	1	1	1			B	B	M			B	B	M		
[E.2] Errores del administrador	MB	1	1	1			B	B	M			MB	MB	B		
[E.8] Difusión de software dañino	B	10	100	10			M	A	A			M	A	A		
[E.9] Errores de re-encaminamiento	MB		10					M					B			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental de la información	MB	1					B					MB				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	MB		1					B					MB			
[E.20] Vulnerabilidades de los programas (software)	B	1	100	1			B	A	M			B	A	M		
[E.21] Errores de mantenimiento / actualización de programas	B	1	1	1			B	B	M			B	B	M		
[A.5] Suplantación de la identidad del usuario	B	1	100		100		B	A		M		B	A		M	
[A.6] Abuso de privilegios de acceso	B	1	10	1			B	M	M			B	M	M		
[A.7] Uso no previsto	B	10	100	10			M	A	A			M	A	A		
[A.8] Difusión de software dañino	MB	10	100	10			M	A	A			MB	M	M		
[A.9] [Re-]encaminamiento de mensajes	MB		10					M					B			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	B	10	100				M	A				M	A			
[A.15] Modificación deliberada de la información	MB	10					M					B				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					A					M			
[A.22] Manipulación de los programas	MB	1	1	1			B	B	M			MB	MB	B		

Tabla 88. Impacto y Riesgo (potencial) del activo SW009- Sistema de backup

[SW] Software		SW009 - Sistema de backup														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		M		A		M		M		A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	MB			10					M					B		
[E.1] Errores de los usuarios	MB	1	1	1			B	MB	B			MB	MB	MB		
[E.2] Errores del administrador	MB	1	1	1			B	MB	B			MB	MB	MB		
[E.8] Difusión de software dañino	MB	10	10	10			M	B	M			B	MB	B		
[E.9] Errores de re-encaminamiento	MB		1					MB					MB			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental de la información	B	1					B					B				
[E.18] Destrucción de la información	MB			10					M					B		
[E.19] Fugas de información	MB		1					MB					MB			
[E.20] Vulnerabilidades de los programas (software)	B	10	100	10			M	M	M			M	M	M		
[E.21] Errores de mantenimiento / actualización de programas	B	10	1	10			M	MB	M			M	MB	M		
[A.5] Suplantación de la identidad del usuario	MB	10	10		100		M	B		M		B	MB		B	
[A.6] Abuso de privilegios de acceso	MB	10	100	10			M	M	M			B	B	B		
[A.7] Uso no previsto	MB	10	100	10			M	M	M			B	B	B		
[A.8] Difusión de software dañino	MB	10	100	100			M	M	A			B	B	M		
[A.9] [Re-]encaminamiento de mensajes	MB		1					MB					MB			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	MB	10	100				M	M				B	B			
[A.15] Modificación deliberada de la información	MB	100					A					M				
[A.18] Destrucción de la información	MB			100					A					M		
[A.19] Divulgación de información	MB		100					M					B			
[A.22] Manipulación de los programas	MB	10	10	10			M	B	M			B	MB	B		

Tabla 89. Impacto y Riesgo (potencial) del activo SW011- Software de fabricación

[SW] Software		SW011 - Software de fabricación														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		B		A		M		A		A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	MB			10					B					MB		
[E.1] Errores de los usuarios	A	10	1	1			B	MB	B			M	B	M		
[E.2] Errores del administrador	M	1	1	10			MB	MB	B			MB	MB	B		
[E.8] Difusión de software dañino	MB	10	10	10			B	MB	B			MB	MB	MB		
[E.9] Errores de re-encaminamiento	MB		1					MB					MB			
[E.10] Errores de secuencia	MB	1					MB					MB				
[E.15] Alteración accidental de la información	A	10					B					M				
[E.18] Destrucción de la información	MB			1					B					MB		
[E.19] Fugas de información	MB		1					MB					MB			
[E.20] Vulnerabilidades de los programas (software)	M	10	1	10			B	MB	B			B	MB	B		
[E.21] Errores de mantenimiento / actualización de programas	M	10	1	10			B	MB	B			B	MB	B		
[A.5] Suplantación de la identidad del usuario	MB	10	100		100		B	B		M		MB	MB		B	
[A.6] Abuso de privilegios de acceso	B	10	10	10			B	MB	B			B	MB	B		
[A.7] Uso no previsto	MB	10	10	10			B	MB	B			MB	MB	MB		
[A.8] Difusión de software dañino	MB	10	10	100			B	MB	A			MB	MB	M		
[A.9] [Re-]encaminamiento de mensajes	MB		10					MB					MB			
[A.10] Alteración de secuencia	MB	1					MB					MB				
[A.11] Acceso no autorizado	MB	10	10				B	MB				MB	MB			
[A.15] Modificación deliberada de la información	M	10					B					B				
[A.18] Destrucción de la información	B			100					A					A		
[A.19] Divulgación de información	B		100					B					B			
[A.22] Manipulación de los programas	MB	10	100	10			B	B	B			MB	MB	MB		

Tabla 90. Impacto y Riesgo (potencial) del activo SW012- Software de gestión de proyectos

[SW] Software		SW012 - Software de gestión de proyectos														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		A		MA		M		A		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	MB			10					A					M		
[E.1] Errores de los usuarios	A	10	1	1			M	B	M			A	M	A		
[E.2] Errores del administrador	M	1	1	10			B	B	A			B	B	A		
[E.8] Difusión de software dañino	MB	10	10	10			M	M	A			B	B	M		
[E.9] Errores de re-encaminamiento	MB		10					M					B			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental de la información	M	10					M					M				
[E.18] Destrucción de la información	M			10					A					A		
[E.19] Fugas de información	MB		10					M					B			
[E.20] Vulnerabilidades de los programas (software)	M	10	10	10			M	M	A			M	M	A		
[E.21] Errores de mantenimiento / actualización de programas	M	10	10	10			M	M	A			M	M	A		
[A.5] Suplantación de la identidad del usuario	B	10	10		100		M	M		M		M	M		M	
[A.6] Abuso de privilegios de acceso	A	10	100	10			M	A	A			A	MA	MA		
[A.7] Uso no previsto	MB	10	100	10			M	A	A			B	M	M		
[A.8] Difusión de software dañino	MB	10	100	100			M	A	MA			B	M	A		
[A.9] [Re-]encaminamiento de mensajes	MB		100					A					M			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	MB	10	100				M	A				B	M			
[A.15] Modificación deliberada de la información	M	100					A					A				
[A.18] Destrucción de la información	B			100					MA					MA		
[A.19] Divulgación de información	B		100					A					A			
[A.22] Manipulación de los programas	MB	10	100	10			M	A	A			B	M	M		

7.3.4. [HW] Hardware (impacto y riesgo potencial)

Tabla 91. Impacto y Riesgo (potencial) del activo HW003- Ordenadores diseño

[HW] Hardware		HW003 - Ordenadores diseño														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		M		A						A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					A					M		
[I.1] Fuego	B			100					A					A		
[I.2] Daños por agua	B			100					A					A		
[I.*] Desastres naturales	MB			100					A					M		
[I.3] Contaminación mecánica	M			10					M					M		
[I.4] Contaminación electromagnética	MB			10					M					B		
[I.5] Avería de origen físico o lógico	B			100					A					A		
[I.6] Corte de suministro eléctrico	MB			100					A					M		
[I.7] Condiciones inadecuadas de temperatura o humedad	B			10					M					M		
[I.11] Emanaciones electromagnéticas	MB			1					B					MB		
[E.2] Errores del administrador	MB	1	10	10			MB	B	M			MB	MB	B		
[E.23] Errores de mantenimiento / actualización de equipos	B			10					M					M		
[E.24] Caída del sistema por agotamiento de recursos	B			1					B					B		
[E.25] Perdida de equipos	MB		100	100				M	A				B	M		
[A.6] Abuso de privilegios de acceso	M	10	10	10			B	B	M			B	B	M		
[A.7] Uso no previsto	M	10	10	10			B	B	M			B	B	M		
[A.11] Acceso no autorizado	M	10	10				B	B				B	B			
[A.23] Manipulación de los equipos	MB	10	10				B	B				MB	MB			
[A.24] Denegación de servicio	MB			100					A					M		
[A.25] Robo	B		100	100				M	A				M	A		
[A.26] Ataque destructivo	MB			100					A					M		

Tabla 92. Impacto y Riesgo (potencial) del activo HW006- NAS

[HW] Hardware		HW006 - NAS														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA						MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					MA					A		
[I.1] Fuego	B			100					MA					MA		
[I.2] Daños por agua	B			100					MA					MA		
[I.*] Desastres naturales	MB			100					MA					A		
[I.3] Contaminación mecánica	M			10					A					A		
[I.4] Contaminación electromagnética	MB			10					A					M		
[I.5] Avería de origen físico o lógico	B			100					MA					MA		
[I.6] Corte de suministro eléctrico	MB			100					MA					A		
[I.7] Condiciones inadecuadas de temperatura o humedad	B			10					A					A		
[I.11] Emanaciones electromagnéticas	MB			1					M					B		
[E.2] Errores del administrador	MB	1	1	10			M	M	A			B	B	M		
[E.23] Errores de mantenimiento / actualización de equipos	B			10					A					A		
[E.24] Caída del sistema por agotamiento de recursos	B			10					A					A		
[E.25] Perdida de equipos	MB		100	100				MA	MA				A	A		
[A.6] Abuso de privilegios de acceso	B	10	100	10			A	MA	A			A	MA	A		
[A.7] Uso no previsto	MB	10	100	10			A	MA	A			M	A	M		
[A.11] Acceso no autorizado	B	10	10				A	A				A	A			
[A.23] Manipulación de los equipos	MB	10	10				A	A				M	M			
[A.24] Denegación de servicio	MB			100					MA					A		
[A.25] Robo	B		100	100				MA	MA				MA	MA		
[A.26] Ataque destructivo	MB			100					MA					A		

Tabla 93. Impacto y Riesgo (potencial) del activo HW007- Router

[HW] Hardware		HW007 - Router														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA						MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					MA					A		
[I.1] Fuego	B			100					MA					MA		
[I.2] Daños por agua	B			100					MA					MA		
[I.*] Desastres naturales	MB			100					MA					A		
[I.3] Contaminación mecánica	M			10					A					A		
[I.4] Contaminación electromagnética	B			10					A					A		
[I.5] Avería de origen físico o lógico	B			100					MA					MA		
[I.6] Corte de suministro eléctrico	MB			100					MA					A		
[I.7] Condiciones inadecuadas de temperatura o humedad	B			100					MA					MA		
[I.11] Emanaciones electromagnéticas	MB			1					M					B		
[E.2] Errores del administrador	B	10	10	10			A	A	A			A	A	A		
[E.23] Errores de mantenimiento / actualización de equipos	B			10					A					A		
[E.24] Caída del sistema por agotamiento de recursos	B			10					A					A		
[E.25] Perdida de equipos	MB		10	100				A	MA				M	A		
[A.6] Abuso de privilegios de acceso	B	100	100	10			MA	MA	A			MA	MA	A		
[A.7] Uso no previsto	MB	10	100	10			A	MA	A			M	A	M		
[A.11] Acceso no autorizado	B	10	100				A	MA				A	MA			
[A.23] Manipulación de los equipos	MB	100	100				MA	MA				A	A			
[A.24] Denegación de servicio	M			100					MA					MA		
[A.25] Robo	B		10	100				A	MA				A	MA		
[A.26] Ataque destructivo	MB			100					MA					A		

Tabla 94. Impacto y Riesgo (potencial) del activo HW009- Servidores físicos

[HW] Hardware		HW009 – Servidores físicos														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA		MA		MA		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					MA					A		
[I.1] Fuego	B			100					MA					MA		
[I.2] Daños por agua	B			100					MA					MA		
[I.*] Desastres naturales	MB			100					MA					A		
[I.3] Contaminación mecánica	M			10					A					A		
[I.4] Contaminación electromagnética	MB			10					A					M		
[I.5] Avería de origen físico o lógico	M			100					MA					MA		
[I.6] Corte de suministro eléctrico	MB			100					MA					A		
[I.7] Condiciones inadecuadas de temperatura o humedad	M			10					A					A		
[I.11] Emanaciones electromagnéticas	MB			1					M					B		
[E.2] Errores del administrador	B	10	10	10			A	A	A			A	A	A		
[E.23] Errores de mantenimiento / actualización de equipos	B			10					A					A		
[E.24] Caída del sistema por agotamiento de recursos	B			10					A					A		
[E.25] Perdida de equipos	MB		100	100				MA	MA				A	A		
[A.6] Abuso de privilegios de acceso	B	10	100	10			A	MA	A			A	MA	A		
[A.7] Uso no previsto	MB	10	100	10			A	MA	A			M	A	M		
[A.11] Acceso no autorizado	B	10	10				A	A				A	A			
[A.23] Manipulación de los equipos	MB	10	10				A	A				M	M			
[A.24] Denegación de servicio	MB			100					MA					A		
[A.25] Robo	B		100	100				MA	MA				MA	MA		
[A.26] Ataque destructivo	MB			100					MA					A		

Tabla 95. Impacto y Riesgo (potencial) del activo HW010- Servidores virtualizados

[HW] Hardware		HW010 - Servidores virtualizados														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		MA		A		MA		A		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					A					M		
[I.1] Fuego	B			100					A					A		
[I.2] Daños por agua	B			100					A					A		
[I.*] Desastres naturales	MB			100					A					M		
[I.3] Contaminación mecánica	M			10					M					M		
[I.4] Contaminación electromagnética	MB			10					M					B		
[I.5] Avería de origen físico o lógico	M			10					M					M		
[I.6] Corte de suministro eléctrico	MB			100					A					M		
[I.7] Condiciones inadecuadas de temperatura o humedad	M			10					M					M		
[I.11] Emanaciones electromagnéticas	MB			1					B					MB		
[E.2] Errores del administrador	M	10	10	1			M	A	B			M	A	B		
[E.23] Errores de mantenimiento / actualización de equipos	M			10					M					M		
[E.24] Caída del sistema por agotamiento de recursos	B			10					M					M		
[E.25] Perdida de equipos	MB		1	1				M	B				B	MB		
[A.6] Abuso de privilegios de acceso	MB	10	100	10			M	MA	M			B	A	B		
[A.7] Uso no previsto	MB	10	100	10			M	MA	M			B	A	B		
[A.11] Acceso no autorizado	B	10	10				M	A				M	A			
[A.23] Manipulación de los equipos	MB	10	10				M	A				B	M			
[A.24] Denegación de servicio	MB			100					A					M		
[A.25] Robo	B		1	100				M	A				M	A		
[A.26] Ataque destructivo	MB			100					A					M		

Tabla 96. Impacto y Riesgo (potencial) del activo HW011- Switch

[HW] Hardware		HW011 - Switch														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		A		MA				A		A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					MA					A		
[I.1] Fuego	B			100					MA					MA		
[I.2] Daños por agua	B			100					MA					MA		
[I.*] Desastres naturales	MB			100					MA					A		
[I.3] Contaminación mecánica	B			10					A					A		
[I.4] Contaminación electromagnética	B			10					A					A		
[I.5] Avería de origen físico o lógico	B			100					MA					MA		
[I.6] Corte de suministro eléctrico	MB			100					MA					A		
[I.7] Condiciones inadecuadas de temperatura o humedad	B			100					MA					MA		
[I.11] Emanaciones electromagnéticas	MB			1					M					B		
[E.2] Errores del administrador	MB	1	1	10			B	B	A			MB	MB	M		
[E.23] Errores de mantenimiento / actualización de equipos	MB			10					A					M		
[E.24] Caída del sistema por agotamiento de recursos	B			10					A					A		
[E.25] Perdida de equipos	MB		1	100				B	MA				MB	A		
[A.6] Abuso de privilegios de acceso	B	10	100	10			M	A	A			M	A	A		
[A.7] Uso no previsto	B	10	100	10			M	A	A			M	A	A		
[A.11] Acceso no autorizado	B	10	100				M	A				M	A			
[A.23] Manipulación de los equipos	MB	100	10				A	M				M	B			
[A.24] Denegación de servicio	MB			100					MA					A		
[A.25] Robo	B		1	100				B	MA				B	MA		
[A.26] Ataque destructivo	MB			100					MA					A		

Tabla 97. Impacto y Riesgo (potencial) del activo HW014- Mini-switch

[HW] Hardware		HW014 – Mini-switch														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		MA		MA				A		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					MA					A		
[I.1] Fuego	B			100					MA					MA		
[I.2] Daños por agua	B			100					MA					MA		
[I.*] Desastres naturales	MB			100					MA					A		
[I.3] Contaminación mecánica	M			10					A					A		
[I.4] Contaminación electromagnética	B			10					A					A		
[I.5] Avería de origen físico o lógico	B			100					MA					MA		
[I.6] Corte de suministro eléctrico	MB			100					MA					A		
[I.7] Condiciones inadecuadas de temperatura o humedad	B			10					A					A		
[I.11] Emanaciones electromagnéticas	MB			1					M					B		
[E.2] Errores del administrador	B	1	1	10			B	M	A			B	M	A		
[E.23] Errores de mantenimiento / actualización de equipos	B			10					A					A		
[E.24] Caída del sistema por agotamiento de recursos	B			100					MA					MA		
[E.25] Perdida de equipos	B		1	100				M	MA				M	MA		
[A.6] Abuso de privilegios de acceso	B	10	100	10			M	MA	A			M	MA	A		
[A.7] Uso no previsto	M	10	100	10			M	MA	A			M	MA	A		
[A.11] Acceso no autorizado	B	10	100				M	MA				M	MA			
[A.23] Manipulación de los equipos	MB	100	10				A	A				M	M			
[A.24] Denegación de servicio	B			100					MA					MA		
[A.25] Robo	B		1	100				M	MA				M	MA		
[A.26] Ataque destructivo	MB			100					MA					A		

Tabla 98. Impacto y Riesgo (potencial) del activo HW016- Terminales

[HW] Hardware		HW016 - Terminales														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		B		A				A		A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					A					M		
[I.1] Fuego	B			100					A					A		
[I.2] Daños por agua	B			100					A					A		
[I.*] Desastres naturales	MB			100					A					M		
[I.3] Contaminación mecánica	M			100					A					A		
[I.4] Contaminación electromagnética	MB			10					M					B		
[I.5] Avería de origen físico o lógico	MB			100					A					M		
[I.6] Corte de suministro eléctrico	MB			100					A					M		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			10					M					B		
[I.11] Emanaciones electromagnéticas	MB			1					B					MB		
[E.2] Errores del administrador	MB	1	1	1			B	MB	B			B	MB	MB		
[E.23] Errores de mantenimiento / actualización de equipos	B			10					M					M		
[E.24] Caída del sistema por agotamiento de recursos	MB			1					B					MB		
[E.25] Perdida de equipos	MB		100	10				B	M				B	B		
[A.6] Abuso de privilegios de acceso	B	10	100	10			M	B	M			M	B	M		
[A.7] Uso no previsto	MB	10	10	10			M	MB	M			M	MB	B		
[A.11] Acceso no autorizado	B	10	10				M	MB				M	MB			
[A.23] Manipulación de los equipos	MB	10	10				M	MB				M	MB			
[A.24] Denegación de servicio	MB			100					A					M		
[A.25] Robo	MB		100	100				B	A				B	M		
[A.26] Ataque destructivo	MB			100					A					M		

Tabla 99. Impacto y Riesgo (potencial) del activo HW018- Servidor de copias

[HW] Hardware		HW018 – Servidor de copias														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		A		A		A		A		A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					A					M		
[I.1] Fuego	B			100					A					A		
[I.2] Daños por agua	B			100					A					A		
[I.*] Desastres naturales	MB			100					A					M		
[I.3] Contaminación mecánica	M			10					M					M		
[I.4] Contaminación electromagnética	MB			10					M					B		
[I.5] Avería de origen físico o lógico	MB			100					A					M		
[I.6] Corte de suministro eléctrico	MB			100					A					M		
[I.7] Condiciones inadecuadas de temperatura o humedad	B			10					M					M		
[I.11] Emanaciones electromagnéticas	MB			1					B					MB		
[E.2] Errores del administrador	MB	10	100	10			M	A	M			B	M	B		
[E.23] Errores de mantenimiento / actualización de equipos	MB			10					M					B		
[E.24] Caída del sistema por agotamiento de recursos	B			10					M					M		
[E.25] Perdida de equipos	MB		100	100				A	A				M	M		
[A.6] Abuso de privilegios de acceso	B	10	100	10			M	A	M			M	A	M		
[A.7] Uso no previsto	MB	10	100	10			M	A	M			B	M	B		
[A.11] Acceso no autorizado	B	10	10				M	M				M	M			
[A.23] Manipulación de los equipos	MB	10	10				M	M				B	B			
[A.24] Denegación de servicio	MB			100					A					M		
[A.25] Robo	B		100	100				A	A				A	A		
[A.26] Ataque destructivo	MB			100					A					M		

7.3.5. [COM] Redes de comunicaciones (impacto y riesgo potencial)

Tabla 100. Impacto y Riesgo (potencial) del activo COM001 – Red local LAN

[COM] Redes de comunicaciones		COM001 – Red local LAN														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA		A		A		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	MB			100					MA					A		
[E.2] Errores del administrador	B	10	10	10			A	A	A			A	A	A		
[E.9] Errores de re-encaminamiento	MB		100					MA					A			
[E.10] Errores de secuencia	MB	10					A					M				
[E.15] Alteración accidental de la información	MB	1					M					B				
[E.18] Destrucción de la información	MB			1					M					B		
[E.19] Fugas de información	MB		10					A					M			
[E.24] Caída del sistema por agotamiento de recursos	B			100					MA					MA		
[A.5] Suplantación de la identidad del usuario	B	10	100		100		A	MA		A		A	MA		A	
[A.6] Abuso de privilegios de acceso	M	10	100	10			A	MA	A			A	MA	A		
[A.7] Uso no previsto	B	10	100	10			A	MA	A			A	MA	A		
[A.9] Re-encaminamiento de mensajes	B		100					MA					MA			
[A.10] Alteración de secuencia	B	10					A					A				
[A.11] Acceso no autorizado	M	10	100				A	MA				A	MA			
[A.12] Análisis de trafico	MB		100					MA					A			
[A.14] Interceptación de información (escucha)	MB		100					MA					A			
[A.15] Modificación deliberada de la información	B	10					A					A				
[A.19] Divulgación de información	M		10					A					A			
[A.24] Denegación de servicio	B			100					MA					MA		

Tabla 101. Impacto y Riesgo (potencial) del activo COM005 – Fibra

[COM] Redes de comunicaciones		COM005 – Fibra														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		MA		MA		A		A		MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	MB			100					MA					A		
[E.2] Errores del administrador	MB	1	1	1			B	M	M			MB	B	B		
[E.9] Errores de re-encaminamiento	MB		100					MA					A			
[E.10] Errores de secuencia	MB	10					M					B				
[E.15] Alteración accidental de la información	MB	1					B					MB				
[E.18] Destrucción de la información	MB			1					M					B		
[E.19] Fugas de información	MB		10					A					M			
[E.24] Caída del sistema por agotamiento de recursos	B			100					MA					MA		
[A.5] Suplantación de la identidad del usuario	MB	10	100		100		M	MA		A		B	A		M	
[A.6] Abuso de privilegios de acceso	MB	1	100	1			B	MA	M			MB	A			
[A.7] Uso no previsto	MB	10	100	10			M	MA	A			B	A	M		
[A.9] Re-encaminamiento de mensajes	MB		100					MA					A			
[A.10] Alteración de secuencia	MB	10					M					B				
[A.11] Acceso no autorizado	MB	1	100				B	MA				MB	A			
[A.12] Análisis de trafico	MB		100					MA					A			
[A.14] Interceptación de información (escucha)	MB		100					MA					A			
[A.15] Modificación deliberada de la información	B	10					M					M				
[A.19] Divulgación de información	M		10					A					A			
[A.24] Denegación de servicio	B			100					MA					MA		

7.3.6. [Media] Soportes de información (impacto y riesgo potencial)

Tabla 102. Impacto y Riesgo (potencial) del activo MEDIA001 – Discos duros extraíbles

[MEDIA] Soportes de información		MEDIA001 – Discos duros extraíbles														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		A						MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					A					M		
[I.1] Fuego	B			100					A					A		
[I.2] Daños por agua	B			100					A					A		
[I.*] Desastres naturales	MB			100					A					M		
[I.3] Contaminación mecánica	M			10					M					M		
[I.4] Contaminación electromagnética	MB			100					A					M		
[I.5] Avería de origen físico o lógico	MB			100					A					M		
[I.6] Corte de suministro eléctrico	MB			100					A					M		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			10					M					B		
[I.10] Degradación de los soportes de almacenamiento	MB			10					M					B		
[I.11] Emanaciones electromagnéticas	MB			1					B					MB		
[E.1] Errores de los usuarios	MB	10	100	10			A	MA	M			M	A	B		
[E.2] Errores del administrador	MB	10	100	100			A	MA	A			M	A	M		
[E.15] Alteración accidental de la información	B	10					A					A				
[E.18] Destrucción de la información	B			100					A					A		
[E.19] Fugas de información	MB		100					MA					A			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B			10					M					M		
[E.25] Perdida de equipos	B		100	100				MA	A				MA	A		
[A.7] Uso no previsto	MB	100	100	100			MA	MA	A			A	A	M		
[A.11] Acceso no autorizado	B	10	10				A	A				A	A			
[A.15] Modificación deliberada de la información	MB	100					MA					A				
[A.18] Destrucción de la información	MB			100					A					M		
[A.19] Divulgación de información	MB		10					A					M			
[A.23] Manipulación de los equipos	MB		1	1				M	B				B	MB		
[A.25] Robo	B		100	100				MA	A				MA	A		
[A.26] Ataque destructivo	MB			100					A					M		

Tabla 103. Impacto y Riesgo (potencial) del activo MEDIA002 – Blue-Ray

[MEDIA] Soportes de información		MEDIA002 – Blue-Ray														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		A		B						A				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					B					MB		
[I.1] Fuego	B			100					B					B		
[I.2] Daños por agua	B			100					B					B		
[I.*] Desastres naturales	MB			100					B					MB		
[I.3] Contaminación mecánica	M			100					B					B		
[I.4] Contaminación electromagnética	MB			100					B					MB		
[I.5] Avería de origen físico o lógico	MB			100					B					MB		
[I.6] Corte de suministro eléctrico	MB			100					B					MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			100					B					MB		
[I.10] Degradación de los soportes de almacenamiento	B			10					MB					MB		
[I.11] Emanaciones electromagnéticas	MB			1					MB					MB		
[E.1] Errores de los usuarios	MB	10	100	10			B	A	MB			MB	M	MB		
[E.2] Errores del administrador	B	10	100	100			B	A	B			B	A	B		
[E.15] Alteración accidental de la información	B	100					M					M				
[E.18] Destrucción de la información	MB			100					B					MB		
[E.19] Fugas de información	B		100					A					A			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MB			10					MB					MB		
[E.25] Perdida de equipos	B		100	100				A	B				A	B		
[A.7] Uso no previsto	MB	100	100	100			M	A	B			B	M	MB		
[A.11] Acceso no autorizado	B	10	100				B	A				B	A			
[A.15] Modificación deliberada de la información	MB	100					M					B				
[A.18] Destrucción de la información	MB			100					B					MB		
[A.19] Divulgación de información	MB		100					A					M			
[A.23] Manipulación de los equipos	MB		1	1				B	MB				MB	MB		
[A.25] Robo	B		100	100				A	B				A	B		
[A.26] Ataque destructivo	MB			100					B					MB		

7.3.7. [L] Instalaciones (impacto y riesgo potencial)

Tabla 104. Impacto y Riesgo (potencial) del activo L001 – Nave principal

[L] Instalaciones		L001 – Nave principal														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA						MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					MA					A		
[I.1] Fuego	MB			100					MA					A		
[I.2] Daños por agua	B			10					A					M		
[I.*] Desastres naturales	MB			10					A					M		
[I.11] Emanaciones electromag.	MB			1					M					B		
[E.15] Alteración accidental	MB	100					MA					A				
[E.18] Destrucción de la información	B			100					MA					MA		
[E.19] Fugas de información	M		10					A					A			
[A.7] Uso no previsto	MB	10	10	10			A	A	A			M	M	M		
[A.11] Acceso no autorizado	B	10	100				A	MA				A	MA			
[A.15] Modificación deliberada	MB	100					MA					A				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					MA					A			
[A.26] Ataque destructivo	MB			100					MA					A		
[A.27] Ocupación enemiga	MB		100	100				MA	MA				A	A		

Tabla 105. Impacto y Riesgo (potencial) del activo L005 – CPD

[L] Instalaciones		L005 – CPD														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA						MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			100					MA					A		
[I.1] Fuego	B			100					MA					MA		
[I.2] Daños por agua	MB			10					A					M		
[I.*] Desastres naturales	MB			10					A					M		
[I.11] Emanaciones electromag.	MB			1					M					B		
[E.15] Alteración accidental	MB	10					A					M				
[E.18] Destrucción de la información	B			100					MA					MA		
[E.19] Fugas de información	B		10					A					A			
[A.7] Uso no previsto	B	10	10	10			A	A	A			A	A	A		
[A.11] Acceso no autorizado	M	10	100				A	MA				A	MA			
[A.15] Modificación deliberada	MB	10					A					M				
[A.18] Destrucción de la información	MB			100					MA					A		
[A.19] Divulgación de información	MB		100					MA					A			
[A.26] Ataque destructivo	MB			100					MA					A		
[A.27] Ocupación enemiga	MB		100	100				MA	MA				A	A		

7.3.8. [P] Personal (impacto y riesgo potencial)

Tabla 106. Impacto y Riesgo (potencial) del activo P001 – Gerencia

[P] Personal		P001 – Gerencia														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA						MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.19] Fugas de información	M		100					MA					MA			
[E.28] Indisponibilidad del personal	M			100					MA					MA		
[A.28] Indisponibilidad del personal	B			100					MA					MA		
[A.29] Extorsión	MB	100	100	100			MA	MA	MA			A	A	A		
[A.30] Ingeniería social (picaresca)	B	100	100	100			MA	MA	MA			MA	MA	MA		

Tabla 107. Impacto y Riesgo (potencial) del activo P002 – Oficina

[P] Personal		P002 – Oficina														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		MA		M						MA				
Amenazas	Probabilidad	Degradación					Impacto potencial					Riesgo potencial				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.19] Fugas de información	M		100					MA					MA			
[E.28] Indisponibilidad del personal	M			100					M					M		
[A.28] Indisponibilidad del personal	B			10					B					B		
[A.29] Extorsión	MB	10	100	10			B	MA	B			MB	A	MB		
[A.30] Ingeniería social (picaresca)	B	10	100	100			B	MA	M			B	MA	M		

7.4. Determinación de salvaguardas

Ahora que disponemos del cálculo del impacto y riesgo potencial, podemos conocer aquellos activos que presentan un riesgo mayor. Con el objetivo de reducir la probabilidad del riesgo y acotar la degradación en el caso de que la amenaza se materialice, se evaluará la aplicación de posibles salvaguardas o contramedidas sobre los activos y sus dimensiones en riesgo.

En el libro II de la metodología Magerit V3 [10], se nos ofrece un catálogo de salvaguardas que emplearemos en el proceso, de las cuales excluiremos aquellas que no consideremos apropiadas para proteger la dimensión adecuada o no protejan lo suficiente contra las amenazas y aquellas cuya aplicación sea desproporcionada ante el riesgo existente. Por lo tanto, simplemente nos ceñiremos a tratar de reducir los riesgos más críticos para el sistema.

Tras la selección de las salvaguardas, volveremos a realizar el cálculo del impacto y riesgo con las salvaguardas ya aplicadas. En esta ocasión, teniendo en cuenta la disminución sobre el valor de degradación o de probabilidad producida por la aplicación de la salvaguarda, el impacto y el riesgo pasan a considerarse residuales.

Si los cálculos del impacto y riesgo residuales presentan unos valores despreciables, podremos considerar que la eficacia de la contramedida ha sido exitosa y podremos incorporarla en los futuros planes de seguridad a desarrollar.

A continuación, detallamos las fichas para cada activo de los que hemos seleccionado que requieren la aplicación de una salvaguarda, con el impacto y riesgo residuales.

Para ello contamos con el siguiente modelo de ficha, esta se encuentra detallada por dimensiones de valoración. Las frecuencias o dimensiones coloreadas de verde, reflejaran el efecto de la salvaguarda.

Tabla 108. Ejemplo ficha de cálculo impacto/riesgo residual por activo (Elaboración propia)

[D] Datos / Información		**D001 - Documentación y datos**															
Valor		**[I]**		**[C]**		**[D]**		**[A]**		**[T]**		**TOTAL**					
		-		-		-		-		-		-					
Salvaguardas aplicadas		**[COD. SALVAGUARDA] Nombre salvaguarda => [Amenaza o dimensión a la que afecta]**															
Amenazas	**Probabilidad residual**	**Degradación residual**					**Impacto residual**					**Riesgo residual**					
	Frecuencia	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**
[COD.] Descripción amenaza	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

7.4.1. [D] Datos / Información (impacto y riesgo residual)

Tabla 109. Salvaguardas. Impacto y Riesgo (residual) del activo D001-Documentación y datos

[D] Datos / Información		D001 - Documentación y datos														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		A		MA		MA		MA		MA				
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [D.C] Cifrado información => [C]						[D.A] Copias de seguridad de los datos (backup) => [D], [E.18] y [A.18] [D.I] Aseguramiento integridad => [I] [PS.AT] Formación y concienciación Política de Seguridad => [E.1] y Apoyo								
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	M	1	1	1			B	B	M			B	B	M		
[E.2] Errores del administrador	MB	1	1	1			B	B	M			MB	MB	B		
[E.15] Alteración accidental de la información	M	1					B					B				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	B		10					M					M			
[A.5] Suplantación de la identidad del usuario	MB	1	10		10		B	M		A		MB	B		M	
[A.6] Abuso de privilegios de acceso	M	1	10	1			B	M	M			B	M	M		
[A.11] Acceso no autorizado	MB	1	10				B	M				MB	B			
[A.15] Modificación deliberada de la información	M	10					M					M				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	B		10					M					M			

Tabla 110. Salvaguardas. Impacto y Riesgo (residual) del activo D002-Archivo clientes

[D] Datos / Información		D002-Archivo clientes														
Valor		[I]	[C]	[D]	[A]	[T]	TOTAL									
		MA	MA	MA	MA	MA	MA									
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [D.C] Cifrado información => [C]					[D.A] Copias de seguridad de los datos (backup) => [D], [E.18] y [A.18] [D.I] Aseguramiento integridad => [I] [PS.AT] Formación y concienciación Política de Seguridad => [E.1] y Apoyo									
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	B	1	1	1			M	M	M			M	M	M		
[E.2] Errores del administrador	MB	1	1	1			M	M	M			B	B	B		
[E.15] Alteración accidental de la información	M	1					M					M				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	MB		1					M					B			
[A.5] Suplantación de la identidad del usuario	MB	1	10		10		M	A		A		B	M		M	
[A.6] Abuso de privilegios de acceso	B	1	10	1			M	A	M			M	A	M		
[A.11] Acceso no autorizado	MB	1	10				M	A				B	M			
[A.15] Modificación deliberada de la información	M	10					A					A				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	B		10					A					A			

Tabla 111. Salvaguardas. Impacto y Riesgo (residual) del activo D005-Copias de seguridad

[D] Datos / Información		D005-Copias de seguridad														
Valor		[I]	[C]	[D]	[A]	[T]	TOTAL									
		A	A	A	A	M	A									
Salvaguardas aplicadas		[H.AC] Ctrl acceso lógico => [A.11] [D.C] Cifrado información => [C] [BC] Continuidad del negocio => [E.2]					[D.I] Aseguramiento integridad => [I] Política de Seguridad => [E.1] y Apoyo									
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			B	B	B			MB	MB	MB		
[E.2] Errores del administrador	MB	10	1	10			M	B	M			B	MB	B		
[E.15] Alteración accidental de la información	MB	1					B					MB				
[E.18] Destrucción de la información	MB			100					A					M		
[E.19] Fugas de información	MB		1					B					MB			
[A.5] Suplantación de la identidad del usuario	MB	1	10		10		B	M		M		MB	B		B	
[A.6] Abuso de privilegios de acceso	MB	1	1	10			B	B	M			MB	MB	B		
[A.11] Acceso no autorizado	MB	1	10				B	M				MB	B			
[A.15] Modificación deliberada de la información	MB	10					M					B				
[A.18] Destrucción de la información	MB			100					A					M		
[A.19] Divulgación de información	MB		10					M					B			

Tabla 112. Salvaguardas. Impacto y Riesgo (residual) del activo D006-Ficheros de LOG

[D] Datos / Información		D006-Ficheros de LOG														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		M		A		M		M		A				
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [H.tools.LA] Herramienta análisis logs => [I], apoyo						[D.A] Copias de seguridad de los datos (backup) => [D], [E.18] y [A.18] Política de Seguridad => [E.1] y Apoyo								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual		
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			MB	MB	B			MB	MB	MB		
[E.2] Errores del administrador	MB	1	10	1			MB	B	B			MB	MB	MB		
[E.15] Alteración accidental de la información	MB	1					MB					MB				
[E.18] Destrucción de la información	MB			1					B					MB		
[E.19] Fugas de información	MB		1					MB					MB			
[A.5] Suplantación de la identidad del usuario	MB	1	100		10		MB	M		B		MB	B		MB	
[A.6] Abuso de privilegios de acceso	MB	1	10	1			MB	B	B			MB	MB	MB		
[A.11] Acceso no autorizado	MB	1	100				MB	M				MB	B			
[A.15] Modificación deliberada de la información	MB	10					B					MB				
[A.18] Destrucción de la información	MB			10					M					B		
[A.19] Divulgación de información	MB		100					M					B			

Tabla 113. Salvaguardas. Impacto y Riesgo (residual) del activo D007-Ficheros de configuración

[D] Datos / Información		D007-Ficheros de configuración														
Valor		[I]	[C]	[D]	[A]	[T]	TOTAL									
		MA	A	MA	A	MA	A									
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [H.tools.CC] Herramienta de chequeo de configuración => [I], [E.2], [E.15]					[D.A] Copias de seguridad de los datos (backup) => [D], [E.18] y [A.18] [D.I] Aseguramiento integridad => [I] Política de Seguridad => Apoyo									
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	B	M			B	MB	B		
[E.2] Errores del administrador	MB	1	10	1			M	M	M			B	B	B		
[E.15] Alteración accidental de la información	MB	1					M					B				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	MB		10					M					B			
[A.5] Suplantación de la identidad del usuario	MB	1	100		10		M	A		M		B	M		B	
[A.6] Abuso de privilegios de acceso	MB	1	10	1			M	M	M			B	B	B		
[A.11] Acceso no autorizado	MB	1	100				M	A				B	M			
[A.15] Modificación deliberada de la información	MB	10					A					M				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		100					A					M			

Tabla 114. Salvaguardas. Impacto y Riesgo (residual) del activo D008-Base de datos del ERP

[D] Datos / Información		D008-Base de datos del ERP														
Valor		[I]	[C]	[D]	[A]	[T]	TOTAL									
		MA	MA	MA	MA	MA	MA									
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [D.C] Cifrado información => [C]					[D.A] Copias de seguridad de los datos (backup) => [D], [E.18] y [A.18] [D.I] Aseguramiento integridad => [I] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [E.1] y Apoyo									
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	M	M			B	B	B		
[E.2] Errores del administrador	MB	1	1	1			M	M	M			B	B	B		
[E.15] Alteración accidental de la información	MB	1					M					B				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	MB		1					M					B			
[A.5] Suplantación de la identidad del usuario	MB	1	10		10		M	A		A		B	M		M	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			M	M	M			B	B	B		
[A.11] Acceso no autorizado	MB	1	10				M	A				B	M			
[A.15] Modificación deliberada de la información	MB	10					A					M				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		10					A					M			

Tabla 115. Salvaguardas. Impacto y Riesgo (residual) del activo D009-BD del gestor de proyectos

[D] Datos / Información		D009-BD del gestor de proyectos														
Valor		[I]	[C]	[D]	[A]	[T]	TOTAL									
		MA	A	MA	MA	A	MA									
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [D.C] Cifrado información => [C]					[D.A] Copias de seguridad de los datos (backup) => [D], [E.18] y [A.18] [D.I] Aseguramiento integridad => [I] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [E.1] y Apoyo									
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	B	M			B	MB	B		
[E.2] Errores del administrador	MB	10	1	1			A	B	M			M	MB	B		
[E.15] Alteración accidental de la información	B	1					B					B				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	MB		1					B					MB			
[A.5] Suplantación de la identidad del usuario	MB	1	10		10		M	M		A		B	B		M	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			M	B	M			B	MB	B		
[A.11] Acceso no autorizado	MB	1	10				M	M				B	B			
[A.15] Modificación deliberada de la información	MB	10					A					M				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		10					M					B			

Tabla 116. Salvaguardas. Impacto y Riesgo (residual) del activo D010- Datos personal empresa

[D] Datos / Información		D010- Datos personal empresa														
Valor		[I]	[C]	[D]	[A]	[T]	TOTAL									
		A	MA	A	MA	MA	MA									
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [D.C] Cifrado información => [C]			[D.A] Copias de seguridad de los datos (backup) => [D], [E.18] y [A.18] [D.I] Aseguramiento integridad => [I] [PS.AT] Formación y concienciación Política de Seguridad => [E.1] y Apoyo											
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	B	1	1	1			B	M	B			B	M	B		
[E.2] Errores del administrador	MB	1	1	1			B	M	B			MB	B	MB		
[E.15] Alteración accidental de la información	M	1					B					B				
[E.18] Destrucción de la información	MB			10					M					B		
[E.19] Fugas de información	MB		1					M					B			
[A.5] Suplantación de la identidad del usuario	MB	1	10		10		B	A		A		MB	M		M	
[A.6] Abuso de privilegios de acceso	B	1	10	1			B	A	B			B	A	B		
[A.11] Acceso no autorizado	MB	1	10				B	A				MB	M			
[A.15] Modificación deliberada de la información	MB	10					M					B				
[A.18] Destrucción de la información	MB			10					M					B		
[A.19] Divulgación de información	MB		10					A					M			

7.4.2. [S] Servicios (impacto y riesgo residual)

Tabla 117. Salvaguardas. Impacto y Riesgo (residual) del activo S003-VPN

[S] Servicios		S003 - VPN														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		MA		M		A		A		A				
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] , [A.13] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [S.A] Aseguramiento de la disponibilidad => [D]						[S.SC] Se aplican perfiles de seguridad => [C] [BC] Continuidad del negocio => [E.2] [H.tools.TM] Herramienta de monitorización de tráfico => [I] Política de Seguridad => [E.1] y Apoyo								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual		
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			B	M	MB			MB	B	MB		
[E.2] Errores del administrador	B	1	1	1			B	M	MB			B	M	MB		
[E.9] Errores de re-encaminamiento	MB		10					A					M			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental	MB	1					B					MB				
[E.18] Destrucción de la información	MB			1					MB					MB		
[E.19] Fugas de información	MB		1					M					B			
[E.24] Caída del sistema por agotamiento de recursos	B			1					MB					MB		
[A.5] Suplantación identidad	MB	1	1		100		B	M		A					M	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			B	M	MB			MB	B	MB		
[A.7] Uso no previsto	MB	1	1	1			B	M	MB			MB	B	MB		
[A.9] Re-encaminamiento mensajes	MB		10					A					M			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	MB	1	10				B	A				MB	M			
[A.13] Repudio	MB	1				100	B				A	MB				M
[A.15] Modificación deliberada	MB	1					B					MB				
[A.18] Destrucción de la información	MB			1					MB					MB		
[A.19] Divulgación de información	MB		10					A					M			
[A.24] Denegación de servicio	MB			10					B					MB		

Tabla 118. Salvaguardas. Impacto y Riesgo (residual) del activo S004- Virtualización servidores

[S] Servicios		S004 - Virtualización servidores														
Valor		[I]	[C]	[D]	[A]	[T]	TOTAL									
		M	M	A	M	A	A									
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] , [A.13] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [S.A] Aseguramiento de la disponibilidad => [D]					[S.SC] Se aplican perfiles de seguridad => [C] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [E.1] y Apoyo									
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			MB	MB	B			MB	MB	MB		
[E.2] Errores del administrador	B	10	1	1			B	MB	B			B	MB	B		
[E.9] Errores de re-encaminamiento	MB		1					MB					MB			
[E.10] Errores de secuencia	MB	1					MB					MB				
[E.15] Alteración accidental	MB	10					B					MB				
[E.18] Destrucción de la información	MB			1					B					MB		
[E.19] Fugas de información	MB		1					MB					MB			
[E.24] Caída del sistema por agotamiento de recursos	B			1					B					B		
[A.5] Suplantación identidad	MB	1	10		10		MB	B		B		MB	MB		MB	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			MB	MB	B			MB	MB	MB		
[A.7] Uso no previsto	MB	10	1	1			B	MB	B			MB	MB	MB		
[A.9] Re-encaminamiento mensajes	MB		1					MB					MB			
[A.10] Alteración de secuencia	MB	1					MB					MB				
[A.11] Acceso no autorizado	MB	10	10				B	B				MB	MB			
[A.13] Repudio	MB	10				100	B				A	MB				M
[A.15] Modificación deliberada	MB	10					B					MB				
[A.18] Destrucción de la información	MB			1					B					MB		
[A.19] Divulgación de información	MB		10					B					MB			
[A.24] Denegación de servicio	MB			10					M					B		

Tabla 119. Salvaguardas. Impacto y Riesgo (residual) del activo S007-DNS

[S] Servicios		S007 - DNS														
Valor		**[I]**		**[C]**		**[D]**		**[A]**		**[T]**		**TOTAL**				
		A		MB		MA		A		B		MA				
Salvaguardas aplicadas		**[H.AU] Registro, auditoría => [A.6] , [A.13]** **[H.AC] Ctrl acceso lógico => [A.11]** **[H.IA] Identif, autenticac. => [A.5]** **[S.A] Aseguramiento de la disponibilidad => [D]**						**[S.SC] Se aplican perfiles de seguridad => [C]** **[S.dns] Protección del servidor DNS => Apoyo** **[BC] Continuidad del negocio => [E.2]** **Política de Seguridad => [E.1] y Apoyo**								
Amenazas	**Probabilidad residual**	**Degradación residual**					**Impacto residual**					**Riesgo residual**				
	Frecuencia	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**
[E.1] Errores de los usuarios	**MB**	1	1	1			B	MB	M			MB	MB			
[E.2] Errores del administrador	**MB**	1	1	1			B	MB	M				MB			
[E.9] Errores de re-encaminamiento	MB		10					MB					MB			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental	MB	1					B					MB				
[E.18] Destrucción de la información	MB			1					M					B		
[E.19] Fugas de información	MB		1					MB					MB			
[E.24] Caída del sistema por agotamiento de recursos	B			1					M					M		
[A.5] Suplantación identidad	**MB**	1	10		100		B	MB		A		MB	MB		M	
[A.6] Abuso de privilegios de acceso	**MB**	1	1	1			B	MB	M			MB	MB	B		
[A.7] Uso no previsto	MB	10	1	1			M	MB	M			B	MB	B		
[A.9] Re-encaminamiento mensajes	MB		10					MB					MB			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	**MB**	10	10				M	MB				B	MB			
[A.13] Repudio	**MB**	10				100	M				B	B				MB
[A.15] Modificación deliberada	MB	10					M					B				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		10					MB					MB			
[A.24] Denegación de servicio	MB			10					A					M		

Tabla 120. Salvaguardas. Impacto y Riesgo (residual) del activo S009- Active Directory

[S] Servicios		S009 - Active Directory														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		A		MA		M		A		MA				
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] , [A.13] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [S.A] Aseguramiento de la disponibilidad => [D]						[S.SC] Se aplican perfiles de seguridad => [C] [S.dir] Protección del directorio => [T] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [E.1] y Apoyo								
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			MB	B	M			MB	MB	B		
[E.2] Errores del administrador	B	10	1	1			B	B	M			B	B	M		
[E.9] Errores de re-encaminamiento	MB		1					B					MB			
[E.10] Errores de secuencia	MB	1					MB					MB				
[E.15] Alteración accidental	MB	1					MB					MB				
[E.18] Destrucción de la información	MB			1					M					B		
[E.19] Fugas de información	MB		1					B					MB			
[E.24] Caída del sistema por agotamiento de recursos	B			1					M					M		
[A.5] Suplantación identidad	B	1	10		100		MB	M		M		MB	M		M	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			MB	B	M			MB	MB	B		
[A.7] Uso no previsto	MB	10	1	1			B	B	M			MB	MB	B		
[A.9] Re-encaminamiento mensajes	MB		1					B					MB			
[A.10] Alteración de secuencia	MB	1					MB					MB				
[A.11] Acceso no autorizado	MB	10	10				B	M				MB	B			
[A.13] Repudio	MB	10				10	B				M	MB				B
[A.15] Modificación deliberada	MB	100					M					B				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		10					M					B			
[A.24] Denegación de servicio	MB			10					A					M		

Tabla 121. Salvaguardas. Impacto y Riesgo (residual) del activo S010-GPO

[S] Servicios		S010 - GPO														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		M		MA		B		A		MA				
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] , [A.13] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [S.A] Aseguramiento de la disponibilidad => [D]						[S.SC] Se aplican perfiles de seguridad => [C] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [E.1] y Apoyo								
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			B	MB	M			MB	MB	B		
[E.2] Errores del administrador	MB	1	1	1			B	MB	M			MB	MB	B		
[E.9] Errores de re-encaminamiento	MB		1					MB					MB			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental	MB	1					B					MB				
[E.18] Destrucción de la información	MB			1					M					B		
[E.19] Fugas de información	MB		1					MB					MB			
[E.24] Caída del sistema por agotamiento de recursos	B			1					M					M		
[A.5] Suplantación identidad	MB	1	1		100		B	MB		B		MB	MB		MB	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			B	MB	M			MB	MB	B		
[A.7] Uso no previsto	MB	10	1	1			M	MB	M			B	MB	B		
[A.9] Re-encaminamiento mensajes	MB		1					MB					MB			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	MB	10	10				M	B				B	MB			
[A.13] Repudio	MB	10				10	M				M	B				B
[A.15] Modificación deliberada	MB	10					M					B				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		10					B					MB			
[A.24] Denegación de servicio	MB			10					A					M		

Tabla 122. Salvaguardas. Impacto y Riesgo (residual) del activo S015-Servidor ERP

[S] Servicios		S015 – Servidor ERP														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		A		MA		MA		MA		MA				
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] , [A.13] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [S.A] Aseguramiento de la disponibilidad => [D]						[S.SC] Se aplican perfiles de seguridad => [C] [BC] Continuidad del negocio => [E.2] [S.CM] Gestión de cambios => [I] y [A] Política de Seguridad => [E.1] y Apoyo								
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	B	M			B	MB	B		
[E.2] Errores del administrador	MB	1	1	1			M	B	M			B	MB	B		
[E.9] Errores de re-encaminamiento	MB		10					M					B			
[E.10] Errores de secuencia	MB	1					M					B				
[E.15] Alteración accidental	MB	10					A					M				
[E.18] Destrucción de la información	MB			1					M					B		
[E.19] Fugas de información	MB		1					B					MB			
[E.24] Caída del sistema por agotamiento de recursos	B			1					M					M		
[A.5] Suplantación identidad	MB	1	1		100		M	B		A					M	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			M	B	M			B	MB	B		
[A.7] Uso no previsto	MB	10	1	1			A	B	M			M	MB	M		
[A.9] Re-encaminamiento mensajes	MB		1					B					MB			
[A.10] Alteración de secuencia	MB	1					M					B				
[A.11] Acceso no autorizado	MB	10	10				A	M				M	B			
[A.13] Repudio	MB	10				10	A				A	M				M
[A.15] Modificación deliberada	MB	100					A					M				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		10					M					B			
[A.24] Denegación de servicio	MB			10					A					M		

Tabla 123. Salvaguardas. Impacto y Riesgo (residual) del activo S016-PostgreSQL

[S] Servicios		S016 - PostgreSQL														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		A		MA		MA		MA		MA				
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] , [A.13] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [S.A] Aseguramiento de la disponibilidad => [D]						[S.SC] Se aplican perfiles de seguridad => [C] [BC] Continuidad del negocio => [E.2] [S.CM] Gestión de cambios => [I] y [A] Política de Seguridad => [E.1] y Apoyo								
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	B	M			B	MB	B		
[E.2] Errores del administrador	MB	1	1	1			M	B	A			B	MB	M		
[E.9] Errores de re-encaminamiento	MB		10					M					B			
[E.10] Errores de secuencia	MB	1					M					B				
[E.15] Alteración accidental	MB	1					M					B				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	MB		1					B					MB			
[E.24] Caída del sistema por agotamiento de recursos	B			1					M					M		
[A.5] Suplantación identidad	MB	1	10		10		M	M		A		B	B		M	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			M	B	M			B	MB	B		
[A.7] Uso no previsto	MB	1	1	1			M	B	M			B	MB	B		
[A.9] Re-encaminamiento mensajes	MB		10					M					B			
[A.10] Alteración de secuencia	MB	1					M					B				
[A.11] Acceso no autorizado	MB	1	10				M	M				B	B			
[A.13] Repudio	MB	1				10	M				A	B				M
[A.15] Modificación deliberada	MB	10					A					M				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		10					M					B			
[A.24] Denegación de servicio	MB			10					A					M		

Tabla 124. Salvaguardas. Impacto y Riesgo (residual) del activo S017- Microsoft SQLServer

[S] Servicios		S017 - Microsoft SQLServer														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		A		MA		MA		MA		MA				
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] , [A.13] [H.AC] Ctrl acceso lógico => [A.11] [H.IA] Identif, autenticac. => [A.5] [S.A] Aseguramiento de la disponibilidad => [D]						[S.SC] Se aplican perfiles de seguridad => [C] [BC] Continuidad del negocio => [E.2] [S.CM] Gestión de cambios => [I] y [A] Política de Seguridad => [E.1] y Apoyo								
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.1] Errores de los usuarios	MB	1	1	1			M	B	M			B	MB	B		
[E.2] Errores del administrador	MB	1	1	1			M	B	M			B	MB	B		
[E.9] Errores de re-encaminamiento	MB		10					M					B			
[E.10] Errores de secuencia	MB	1					M					B				
[E.15] Alteración accidental	MB	1					M					B				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	MB		1					B					MB			
[E.24] Caída del sistema por agotamiento de recursos	B			1					M					M		
[A.5] Suplantación identidad	MB	1	10		10		M	M		A		B	B		M	
[A.6] Abuso de privilegios de acceso	MB	1	1	1			M	B	M			B	MB	B		
[A.7] Uso no previsto	MB	1	1	1			M	B	M			B	MB	B		
[A.9] Re-encaminamiento mensajes	MB		10					M					B			
[A.10] Alteración de secuencia	MB	1					M					B				
[A.11] Acceso no autorizado	MB	1	10				M	M				B	B			
[A.13] Repudio	MB	1				10	M				A	B				M
[A.15] Modificación deliberada	MB	10					A					M				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		10					M					B			
[A.24] Denegación de servicio	MB			10					A					M		

7.4.3. [SW] Software (impacto y riesgo residual)

Tabla 125. Salvaguardas. Impacto y Riesgo (residual) del activo SW002-Cliente de correo

[SW] Software		SW002 – Cliente de correo														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		MA		MA		MA		A		A				
Salvaguardas aplicadas		[H.AC] Ctrl acceso lógico => [A.11] [SW] Protección de las Aplicaciones Infor. => [I] [SW.SC] Se aplican perfiles de seguridad => [C] [SW.A] Copias de seguridad (backup) => [D]						[SW.CM] Cambios (actu. y mantenimiento) => [I] [H.tools.AV] Herramienta contra código dañino => [E.8], [A.8] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [E.1], [E.19], [A.19]								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	MB			1						M						B		
[E.1] Errores de los usuarios	MB	1	1	1				B	M	M				MB	B	B		
[E.2] Errores del administrador	MB	1	1	1				B	M	M				MB	B	B		
[E.8] Difusión de software dañino	MB	1	10	1				B	A	M				MB	M	B		
[E.9] Errores de re-encaminamiento	MB		1						M						B			
[E.10] Errores de secuencia	MB	1						B						MB				
[E.15] Alteración accidental de la información	B	1						B						B				
[E.18] Destrucción de la información	MB			1						M						B		
[E.19] Fugas de información	MB		10						A						M			
[E.20] Vulnerabilidades de los programas (software)	MB	1	10	1				B	A	M				MB	M	B		
[E.21] Errores de mantenimiento / actualización de programas	MB	1	1	1				B	M	M				MB	B	B		
[A.5] Suplantación de la identidad del usuario	MB	1	10		100			B	A		MA			MB	M		M	
[A.6] Abuso de privilegios de acceso	MB	1	1	1				B	M	M				MB	B	B		
[A.7] Uso no previsto	MB	1	10	1				B	A	M				MB	M	B		
[A.8] Difusión de software dañino	MB	1	10	1				B	A	M				MB	M	B		
[A.9] [Re-]encaminamiento de mensajes	MB		1						M						B			
[A.10] Alteración de secuencia	MB	1						B						MB				
[A.11] Acceso no autorizado	MB	1	10					B	A					MB	M			
[A.15] Modificación deliberada de la información	MB	10						M						B				
[A.18] Destrucción de la información	MB			10						A						M		
[A.19] Divulgación de información	MB		10						A						M			
[A.22] Manipulación de los programas	MB	1	10	1				B	A	M				MB	M	B		

Tabla 126. Salvaguardas. Impacto y Riesgo (residual) del activo SW005-ERP

[SW] Software		SW005 – ERP														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA		MA		MA		MA				
Salvaguardas aplicadas		[H.AU] Registro, auditoría => [A.6] [H.AC] Ctrl acceso lógico => [A.11] [SW] Protección de las Aplicaciones Infor. => [I] [SW.SC] Se aplican perfiles seguridad => [C], [A] [SW.A] Copias de seguridad (backup) => [D]						[SW.CM] Cambios (actualizacion. y mantenimiento) => [E.20],[E.21] [H.tools.LA] Herramienta análisis logs => [E.15], [A.15] Manuales y procedimiento => [E.2] [PS.AT] Formación y concienciación Política de Seguridad => [E.1], [E.19], [A.19]							
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	B			1						M						M		
[E.1] Errores de los usuarios	B	1	10	1				M	A	M				M	M	M		
[E.2] Errores del administrador	MB	1	1	1				M	M	M				B	B	B		
[E.8] Difusión de software dañino	MB	10	10	10				A	A	A				B	B	B		
[E.9] Errores de re-encaminamiento	MB		1						M						B			
[E.10] Errores de secuencia	MB	1						M						B				
[E.15] Alteración accidental de la información	MB	1						M						B				
[E.18] Destrucción de la información	MB			10						A						M		
[E.19] Fugas de información	MB		10						A						M			
[E.20] Vulnerabilidades de los programas (software)	MB	1	10	1				M	A	M				B	M	B		
[E.21] Errores de mantenimiento / actualización de programas	MB	1	1	1				M	M	M				B	B	B		
[A.5] Suplantación de la identidad del usuario	MB	1	10		10			M	A		A			B	M		M	
[A.6] Abuso de privilegios de acceso	MB	1	10	1				M	A	M				B	B	B		
[A.7] Uso no previsto	MB	1	1	1				M	M	M				B	B	B		
[A.8] Difusión de software dañino	MB	10	10	10				A	A	A				B	B	B		
[A.9] [Re-]encaminamiento de mensajes	MB		1						M						B			
[A.10] Alteración de secuencia	MB	1						M						B				
[A.11] Acceso no autorizado	MB	1	10					M	A					B	B			
[A.15] Modificación deliberada de la información	MB	10						A						M				
[A.18] Destrucción de la información	MB			1						M						B		
[A.19] Divulgación de información	MB		10						A						M			
[A.22] Manipulación de los programas	MB	1	10	1				M	A	M				B	B	B		

Tabla 127. Salvaguardas. Impacto y Riesgo (residual) del activo SW006-Suite de diseño gráfico

[SW] Software		SW006 – Suite de diseño gráfico														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		A		A		M		A		A				
Salvaguardas aplicadas		[H.AC] Ctrl acceso lógico => [A.11] [SW] Protección de las Aplicaciones Infor. => [I] [SW.SC] Se aplican perfiles de seguridad => [C] [SW.A] Copias de seguridad (backup) => [D]						[SW.CM] Cambios (actu. y mantenimiento) => [E.20],[E.21] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [E.1], [E.19], [A.19]								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual		
	Frecuencia	[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	B			1						B					B		
[E.1] Errores de los usuarios	B	1	1	1				MB	B	B			MB	B	B		
[E.2] Errores del administrador	MB	1	1	1				MB	B	B			MB	MB	MB		
[E.8] Difusión de software dañino	MB	1	1	1				MB	B	B			MB	MB	MB		
[E.9] Errores de re-encaminamiento	MB		1						B					MB			
[E.10] Errores de secuencia	MB	1						MB					MB				
[E.15] Alteración accidental de la información	MB	1						MB					MB				
[E.18] Destrucción de la información	MB			1						B					MB		
[E.19] Fugas de información	MB		1						B					MB			
[E.20] Vulnerabilidades de los programas (software)	MB	1	1	1				MB	B	B			MB	MB	MB		
[E.21] Errores de mantenimiento / actualización de programas	MB	1	1	1				MB	B	B			MB	MB	MB		
[A.5] Suplantación de la identidad del usuario	MB	1	1		100			MB	B		M		MB	MB		B	
[A.6] Abuso de privilegios de acceso	MB	1	1	1				MB	B	B			MB	MB	MB		
[A.7] Uso no previsto	B	1	1	10				MB	B	M			MB	B	M		
[A.8] Difusión de software dañino	MB	1	1	1				MB	B	B			MB	MB	MB		
[A.9] [Re-]encaminamiento de mensajes	MB		1						B					MB			
[A.10] Alteración de secuencia	MB	1						MB					MB				
[A.11] Acceso no autorizado	MB	1	1					MB	B				MB	MB			
[A.15] Modificación deliberada de la información	MB	10						B					MB				
[A.18] Destrucción de la información	MB			10						M					B		
[A.19] Divulgación de información	MB		10						M					B			
[A.22] Manipulación de los programas	MB	1	10	1				MB	M				MB	B			

Tabla 128. Salvaguardas. Impacto y Riesgo (residual) del activo SW007-Antivirus

[SW] Software		SW007 – Antivirus														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		B		MA		M		M		MA				
Salvaguardas aplicadas		[H.AC] Ctrl acceso lógico [H.AU] Registro y auditoría [SW] Protección de las Aplicaciones Infor. => [I] [SW.SC] Se aplican perfiles de seguridad => [C]						[SW.CM] Cambios (actu. y mantenimiento) => [I] [SW.A] Copias de seguridad (backup) => [D] [BC] Continuidad del negocio Política de Seguridad								
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	MB			1					M					B		
[E.1] Errores de los usuarios	MB	1	1	1			B	MB	B			MB	MB	MB		
[E.2] Errores del administrador	MB	1	1	1			B	MB	B			MB	MB	MB		
[E.8] Difusión de software dañino	MB	1	1	1			M	MB	M			B	MB	B		
[E.9] Errores de re-encaminamiento	MB		1					MB					MB			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental de la información	MB	1					B					MB				
[E.18] Destrucción de la información	MB			1					M					B		
[E.19] Fugas de información	MB		1					MB					MB			
[E.20] Vulnerabilidades de los programas (software)	MB	10	1	1			A	MB	M			M	MB	B		
[E.21] Errores de mantenimiento / actualización de programas	MB	10	1	1			A	MB	M			M	MB	B		
[A.5] Suplantación de la identidad del usuario	MB	1	1		100		M	MB		M		B	MB		B	
[A.6] Abuso de privilegios de acceso	MB	10	1	1			A	MB	M			M	MB	B		
[A.7] Uso no previsto	MB	1	1	1			M	MB	M			B	MB	B		
[A.8] Difusión de software dañino	MB	1	1	1			M	MB	M			B	MB	B		
[A.9] [Re-]encaminamiento de mensajes	MB		1					MB					MB			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	MB	10	1				A	MB				M	MB			
[A.15] Modificación deliberada de la información	MB	10					A					M				
[A.18] Destrucción de la información	MB			1					M					B		
[A.19] Divulgación de información	MB		1					MB					MB			
[A.22] Manipulación de los programas	MB	1	1	1			B	MB	B			MB	MB	MB		

Tabla 129. Salvaguardas. Impacto y Riesgo (residual) del activo SW008- Sistema operativo

[SW] Software		SW008 – Sistema operativo														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		A		MA		M		A		MA				
Salvaguardas aplicadas		[H.AC] Ctrl acceso lógico => [A.11] [H.AU] Registro, auditoría => [A.6] [H.IA] Identif. y autentic => [A.5] y [A.7] [SW] Protección de las Aplicaciones Infor. => [I] [SW.SC] Se aplican perfiles de seguridad => [C] [SW.A] Copias de seguridad (backup) => [D]						[SW.CM] Cambios (actu. y mantenimiento) => [E.20],[E.21] [H.tools.AV] Herramienta contra código dañino => [E.8], [A.8] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [E.1], [E.19], [A.19]							
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	B			1						M					M		
[E.1] Errores de los usuarios	MB	1	1	1				B	B	M			MB	MB	B		
[E.2] Errores del administrador	MB	1	1	1				B	B	M			MB	MB	B		
[E.8] Difusión de software dañino	MB	1	10	1				B	M	M			MB	B	B		
[E.9] Errores de re-encaminamiento	MB		1						B					MB			
[E.10] Errores de secuencia	MB	1						B					MB				
[E.15] Alteración accidental de la información	MB	1						B					MB				
[E.18] Destrucción de la información	MB			1						M					B		
[E.19] Fugas de información	MB		1						B					MB			
[E.20] Vulnerabilidades de los programas (software)	MB	1	10	1				B	M	M			MB	B	B		
[E.21] Errores de mantenimiento / actualización de programas	MB	1	1	1				B	B	M			MB	MB	B		
[A.5] Suplantación de la identidad del usuario	MB	1	10		100			B	M		M		MB	B		B	
[A.6] Abuso de privilegios de acceso	MB	1	1	1				B	B	M			MB	MB	B		
[A.7] Uso no previsto	MB	1	10	1				B	M	M			MB	B	B		
[A.8] Difusión de software dañino	MB	1	10	1				B	M	M			MB	B	B		
[A.9] [Re-]encaminamiento de mensajes	MB		1						B					MB			
[A.10] Alteración de secuencia	MB	1						B					MB				
[A.11] Acceso no autorizado	MB	1	10					B	M				MB	B			
[A.15] Modificación deliberada de la información	MB	1						B					MB				
[A.18] Destrucción de la información	MB			10						A					M		
[A.19] Divulgación de información	MB		10						M					B			
[A.22] Manipulación de los programas	MB	1	1	1				B	B	M			MB	MB	B		

Tabla 130. Salvaguardas. Impacto y Riesgo (residual) del activo SW009- Sistema de backup

[SW] Software		SW009 – Sistema de backup														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		M		A		M		M		A				
Salvaguardas aplicadas		[D.C] Cifrado de la información => [C] [H.AC] Ctrl acceso lógico => [A.11] [H.tools.LA] Herramienta para análisis de logs => [E.15] [H.tools.AV] Herramienta contra código dañino => [E.8], [A.8]						[SW] Protección de las Aplicaciones Infor. => [I] [SW.SC] Se aplican perfiles de seguridad => [C] [SW.A] Copias de seguridad (backup) => [D] [SW.CM] Cambios (actu. y mantenimiento) => [E.20], [E.21] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [E.1], [E.19], [A.19]								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	MB			1						B						MB		
[E.1] Errores de los usuarios	MB	1	1	1				B	MB	B				MB	MB	MB		
[E.2] Errores del administrador	MB	1	1	1				B	MB	B				MB	MB	MB		
[E.8] Difusión de software dañino	MB	1	1	1				B	MB	B				MB	MB	MB		
[E.9] Errores de re-encaminamiento	MB		1						MB						MB			
[E.10] Errores de secuencia	MB	1						B						MB				
[E.15] Alteración accidental de la información	MB	1						B						MB				
[E.18] Destrucción de la información	MB			1						B						MB		
[E.19] Fugas de información	MB		1						MB						MB			
[E.20] Vulnerabilidades de los programas (software)	MB	1	10	1				B	B	B				MB	MB	MB		
[E.21] Errores de mantenimiento / actualización de programas	MB	1	1	1				B	MB	B				MB	MB	MB		
[A.5] Suplantación de la identidad del usuario	MB	1	1		100			B	MB		M			MB	MB		B	
[A.6] Abuso de privilegios de acceso	MB	1	10	1				B	B	B				MB	MB	MB		
[A.7] Uso no previsto	MB	1	10	1				B	B	B				MB	MB	MB		
[A.8] Difusión de software dañino	MB	1	10	10				B	B	M				MB	MB	B		
[A.9] [Re-]encaminamiento de mensajes	MB		1						MB						MB			
[A.10] Alteración de secuencia	MB	1						B						MB				
[A.11] Acceso no autorizado	MB	1	10					B	B					MB	MB			
[A.15] Modificación deliberada de la información	MB	10						M						B				
[A.18] Destrucción de la información	MB			10						M						B		
[A.19] Divulgación de información	MB		10						B						MB			
[A.22] Manipulación de los programas	MB	1	1	1				B	MB	B				MB	MB	MB		

Tabla 131. Salvaguardas. Impacto y Riesgo (residual) del activo SW011- Software de fabricación

[SW] Software		SW011 – Software de fabricación														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		B		A		M		A		A				
Salvaguardas aplicadas		[H.AC] Ctrl acceso lógico => [A.11] [SW] Protección de las Aplicaciones Infor. => [I] [SW.SC] Se aplican perfiles de seguridad => [C] [SW.A] Copias de seguridad (backup) => [D], [E.18] y [A.18]						[SW.CM] Cambios (actu. y mantenimiento) => [E.20], [E.21] [H.tools.LA] Herramienta análisis logs => [E.15], [A.15] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [E.1], [E.19], [A.19]							
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	MB			1					B					MB		
[E.1] Errores de los usuarios	M	1	1	1			MB	MB	B			MB	MB	B		
[E.2] Errores del administrador	B	1	1	1			MB	MB	B			MB	MB	B		
[E.8] Difusión de software dañino	MB	1	1	1			MB	MB	B			MB	MB	MB		
[E.9] Errores de re-encaminamiento	MB		1					MB					MB			
[E.10] Errores de secuencia	MB	1					MB					MB				
[E.15] Alteración accidental de la información	M	1					MB					MB				
[E.18] Destrucción de la información	MB			1					B					MB		
[E.19] Fugas de información	MB		1					MB					MB			
[E.20] Vulnerabilidades de los programas (software)	B	1	1	1			MB	MB	B			MB	MB	B		
[E.21] Errores de mantenimiento / actualización de programas	B	1	1	1			MB	MB	B			MB	MB	B		
[A.5] Suplantación de la identidad del usuario	MB	1	10		100		MB	MB		M		MB	MB		B	
[A.6] Abuso de privilegios de acceso	B	1	1	1			MB	MB	B			MB	MB	B		
[A.7] Uso no previsto	MB	1	1	1			MB	MB	B			MB	MB	B		
[A.8] Difusión de software dañino	MB	1	1	10			MB	MB	M			MB	MB	B		
[A.9] [Re-]encaminamiento de mensajes	MB		1					MB					MB			
[A.10] Alteración de secuencia	MB	1					MB					MB				
[A.11] Acceso no autorizado	MB	1	1				MB	MB				MB	MB			
[A.15] Modificación deliberada de la información	B	1					MB					MB				
[A.18] Destrucción de la información	B			10					M					M		
[A.19] Divulgación de información	MB		10					MB					MB			
[A.22] Manipulación de los programas	MB	1	10	1			MB	MB	B			MB	MB	B		

Tabla 132. Salvaguardas. Impacto y Riesgo (residual) del activo SW012- Software gestión de proyectos

[SW] Software							SW012 – Software de gestión de proyectos									
Valor		[I]		[C]		[D]	[A]		[T]		TOTAL					
		A		A		MA	M		A		MA					
Salvaguardas aplicadas		[H.AC] Ctrl acceso lógico => [A.11] [H.AU] Registro, auditoría => [A.6] [SW] Protección de las Aplicaciones Infor. => [I] [SW.SC] Se aplican perfiles de seguridad => [C] [SW.A] Copias de seguridad (backup) => [D], [E.18] y [A.18]					[SW.CM] Cambios (actu. y mantenimiento) => [E.20], [E.21] [H.tools.LA] Herramienta análisis logs => [E.15], [A.15] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [E.1], [E.19], [A.19]								
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.5] Avería de origen físico o lógico	MB			1					M					B		
[E.1] Errores de los usuarios	M	1	1	1			B	B	M			B	B	M		
[E.2] Errores del administrador	B	1	1	1			B	B	M			B	B	M		
[E.8] Difusión de software dañino	MB	1	1	1			B	B	M			MB	MB	B		
[E.9] Errores de re-encaminamiento	MB		1					B					MB			
[E.10] Errores de secuencia	MB	1					B					MB				
[E.15] Alteración accidental de la información	MB	1					B					MB				
[E.18] Destrucción de la información	MB			1					M					B		
[E.19] Fugas de información	MB		1					B					MB			
[E.20] Vulnerabilidades de los programas (software)	MB	1	1	1			B	B	M			MB	MB	B		
[E.21] Errores de mantenimiento / actualización de programas	MB	1	1	1			B	B	M			MB	MB	B		
[A.5] Suplantación de la identidad del usuario	B	1	1		100		B	B		M		B	B		B	
[A.6] Abuso de privilegios de acceso	MB	1	10	1			B	M	M			MB	B	B		
[A.7] Uso no previsto	MB	1	10	1			B	M	M			MB	B	B		
[A.8] Difusión de software dañino	MB	1	10	10			B	M	A			MB	B	M		
[A.9] [Re-]encaminamiento de mensajes	MB		10					M					B			
[A.10] Alteración de secuencia	MB	1					B					MB				
[A.11] Acceso no autorizado	MB	1	10				B	M				MB	B			
[A.15] Modificación deliberada de la información	MB	10					M					B				
[A.18] Destrucción de la información	B			10					A					M		
[A.19] Divulgación de información	MB		10					M					B			
[A.22] Manipulación de los programas	MB	1	10	1			B	M	M			MB	B	B		

7.4.4. [HW] Hardware (impacto y riesgo residual)

Tabla 133. Salvaguardas. Impacto y Riesgo (residual) del activo HW003- Ordenadores de diseño

[HW] Hardware		HW003 – Ordenadores de diseño														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		M		A						A				
Salvaguardas aplicadas		[D.A] Copias de seguridad de los datos => [D] [H.AC] Ctrl acceso lógico => [A.11], [C] [L.AC] Control acceso físico => [C], [A.7],[A.25] [H.AU] Registro, auditoría => [A.6] [HW] Protección Equipos Informáticos => [I]						[HW.A] Aseguramiento de la disponibilidad => [D] [HW.CM] Cambios (actualizaciones y mantenimiento) => [E.23], [E.24], [I.*] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [A.7]							
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			10					M					MB		
[I.1] Fuego	B			10					M					M		
[I.2] Daños por agua	B			10					M					M		
[I.*] Desastres naturales	MB			10					M					MB		
[I.3] Contaminación mecánica	M			1					B					B		
[I.4] Contaminación electromagnética	MB			1					B					MB		
[I.5] Avería de origen físico o lógico	MB			10					M					B		
[I.6] Corte de suministro eléctrico	MB			10					M					B		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			1					B					MB		
[I.11] Emanaciones electromagnéticas	MB			1					B					MB		
[E.2] Errores del administrador	MB	1	1	1			MB	MB	B			MB	MB	MB		
[E.23] Errores de mantenimiento / actualización de equipos	MB			1					B					MB		
[E.24] Caída del sistema por agotamiento de recursos	MB			1					B					MB		
[E.25] Perdida de equipos	MB		10	10				B	M				MB	B		
[A.6] Abuso de privilegios de acceso	B	1	1	1			MB	MB	B			MB	MB	B		
[A.7] Uso no previsto	B	1	1	1			MB	MB	B			MB	MB	B		
[A.11] Acceso no autorizado	B	1	1				MB	MB				MB	MB			
[A.23] Manipulación de los equipos	MB	1	1				MB	MB				MB	MB			
[A.24] Denegación de servicio	MB			10					M					B		
[A.25] Robo	MB		10	10				B	M				MB	B		
[A.26] Ataque destructivo	MB			10					M					B		

Tabla 134. Salvaguardas. Impacto y Riesgo (residual) del activo HW006- NAS

[HW] Hardware	HW006 – NAS															
Valor	[I]		[C]		[D]		[A]			[T]		TOTAL				
	MA		MA		MA							MA				
Salvaguardas aplicadas	[D.A] Copias de seguridad de los datos => [D] [H.AC] Ctrl acceso lógico => [A.11], [C] [L.AC] Control acceso físico => [C], [A.7],[A.25] [H.AU] Registro, auditoría => [A.6] [HW] Protección Equipos Informáticos => [I] [D.C] Cifrado información => [C]						[HW.A] Aseguramiento de la disponibilidad => [D] [HW.CM] Cambios (actualizaciones y mantenimiento) => [E.23], [E.24], [I.*] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [A.7] CPD Dedicado [I.1], [I.2], [I.3], [I.7], [I.*]								
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			10					A					M		
[I.1] Fuego	MB			10					A					M		
[I.2] Daños por agua	MB			10					A					M		
[I.*] Desastres naturales	MB			10					A					M		
[I.3] Contaminación mecánica	MB			1					M					B		
[I.4] Contaminación electromagnética	MB			1					M					B		
[I.5] Avería de origen físico o lógico	MB			10					A					M		
[I.6] Corte de suministro eléctrico	MB			10					A					M		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			1					M					B		
[I.11] Emanaciones electromagnéticas	MB			1					M					B		
[E.2] Errores del administrador	MB	1	1	1			M	M	M			B	B	B		
[E.23] Errores de mantenimiento / actualización de equipos	MB			1					M					B		
[E.24] Caída del sistema por agotamiento de recursos	MB			1					M					B		
[E.25] Perdida de equipos	MB		10	10				A	A				M	M		
[A.6] Abuso de privilegios de acceso	MB	1	10	1			M	A	M			B	M	B		
[A.7] Uso no previsto	MB	1	10	1			M	A	M			B	M	B		
[A.11] Acceso no autorizado	MB	1	1				M	M				B	B			
[A.23] Manipulación de los equipos	MB	1	1				M	M				B	B			
[A.24] Denegación de servicio	MB			10					A					M		
[A.25] Robo	MB		10	10				A	A				M	M		
[A.26] Ataque destructivo	MB			10					A					M		

Tabla 135. Salvaguardas. Impacto y Riesgo (residual) del activo HW007- Router

[HW] Hardware	HW007 – Router															
Valor		**[I]**		**[C]**		**[D]**		**[A]**		**[T]**		**TOTAL**				
		MA		MA		MA						MA				
Salvaguardas aplicadas		**[SW.A] Copia de seguridad configuración => [D]** **[H.AC] Ctrl acceso lógico => [A.11], [C]** **[L.AC] Control acceso físico => [C], [A.7],[A.25]** **[H.IA] Identificación y autenticación => [C]** **[HW] Protección Equipos Informáticos => [I]**						**[HW.A] Aseguramiento disponibilidad => [D], [A.24]** **[HW.CM] Cambios (actualizaciones y mantenimiento) => [E.23], [E.24], [I.*]** **[BC] Continuidad del negocio => [E.2]** **Política de Seguridad** **CPD Dedicado [I.1], [I.2], [I.3], [I.7], [I.*]**							
Amenazas	**Probabilidad residual**	**Degradación residual**						**Impacto residual**						**Riesgo residual**		
	Frecuencia	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**	**[I]**	**[C]**	**[D]**	**[A]**	**[T]**
[N] Desastres naturales	MB			10					A					M		
[I.1] Fuego	**MB**			10					A					M		
[I.2] Daños por agua	**MB**			10					A					M		
[I.*] Desastres naturales	**MB**			10					A					M		
[I.3] Contaminación mecánica	**MB**			1					M					B		
[I.4] Contaminación electromagnética	**MB**			1					M					B		
[I.5] Avería de origen físico o lógico	**MB**			10					A					M		
[I.6] Corte de suministro eléctrico	MB			10					A					M		
[I.7] Condiciones inadecuadas de temperatura o humedad	**MB**			10					A					M		
[I.11] Emanaciones electromagnéticas	MB			1					B					MB		
[E.2] Errores del administrador	**MB**	1	1	1			M	M	M			B	B	B		
[E.23] Errores de mantenimiento / actualización de equipos	**MB**			1					M					B		
[E.24] Caída del sistema por agotamiento de recursos	**MB**			1					M					B		
[E.25] Perdida de equipos	MB		1	10				M	A				B	M		
[A.6] Abuso de privilegios de acceso	**MB**	10	10	1			A	A	M			M	M	B		
[A.7] Uso no previsto	**MB**	1	10	1			M	A	M			B	B	B		
[A.11] Acceso no autorizado	**MB**	1	10				M	A				B	B			
[A.23] Manipulación de los equipos	MB	10	10				A	A				M	M			
[A.24] Denegación de servicio	**MB**			10					A					M		
[A.25] Robo	**MB**		1	10				M	A				B	M		
[A.26] Ataque destructivo	MB			10					A					M		

Tabla 136. Salvaguardas. Impacto y Riesgo (residual) del activo HW009- Servidores físicos

[HW] Hardware	HW009 – Servidores físicos					
Valor	[I]	[C]	[D]	[A]	[T]	TOTAL
	MA	MA	MA	MA	MA	MA
Salvaguardas aplicadas	[D.A] Copias de seguridad de los datos => [D] [H.AC] Ctrl acceso lógico => [A.11], [C] [L.AC] Control acceso físico => [C], [A.7],[A.25] [H.AU] Registro, auditoría => [A.6] [HW] Protección Equipos Informáticos => [I] [D.C] Cifrado información => [C] [H.tools.LA] Herramienta análisis logs => [E.15], [A.15]			[H.tools.AV] Herramienta contra código dañino => [E.8], [A.8] [HW.A] Aseguramiento de la disponibilidad => [D] [HW.CM] Cambios (actualizaciones y mantenimiento) => [E.23], [E.24], [I.*] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [A.7] CPD Dedicado [I.1], [I.2], [I.3], [I.7], [I.*]		

Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			10					A					M		
[I.1] Fuego	MB			10					A					M		
[I.2] Daños por agua	MB			10					A					M		
[I.*] Desastres naturales	MB			10					A					M		
[I.3] Contaminación mecánica	MB			1					M					B		
[I.4] Contaminación electromagnética	MB			1					M					B		
[I.5] Avería de origen físico o lógico	MB			10					A					M		
[I.6] Corte de suministro eléctrico	MB			10					A					M		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			1					M					B		
[I.11] Emanaciones electromagnéticas	MB			1					M					B		
[E.2] Errores del administrador	MB	1	1	1			M	M	M			B	B	B		
[E.23] Errores de mantenimiento / actualización de equipos	MB			1					M					B		
[E.24] Caída del sistema por agotamiento de recursos	MB			1					M					B		
[E.25] Perdida de equipos	MB		10	10				A	A				M	M		
[A.6] Abuso de privilegios de acceso	MB	1	10	1			M	A	M			B	M	B		
[A.7] Uso no previsto	MB	1	10	1			M	A	M			B	M	B		
[A.11] Acceso no autorizado	MB	1	1				M	M				B	B			
[A.23] Manipulación de los equipos	MB	1	1				M	M				B	B			
[A.24] Denegación de servicio	MB			10					A					M		
[A.25] Robo	MB		10	10				A	A				M	M		
[A.26] Ataque destructivo	MB			10					A					M		

Tabla 137. Salvaguardas. Impacto y Riesgo (residual) del activo HW010- Servidores virtualizados

[HW] Hardware		HW010 – Servidores virtualizados														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		MA		A		MA		A		MA				
Salvaguardas aplicadas		[D.A] Copias de seguridad de los datos => [D] [H.AC] Ctrl acceso lógico => [A.11], [C] [H.AU] Registro, auditoría => [A.6] [H.tools.LA] Herramienta análisis logs => [E.15], [A.15] Equipos virtualizados => [N], [I.*]						[H.tools.AV] Herramienta contra código dañino => [E.8], [A.8] [HW.A] Aseguramiento de la disponibilidad => [D] [HW.CM] Cambios (actualizaciones y mantenimiento) => [E.23], [E.24], [I.*] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [A.7]							
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			1					M					B		
[I.1] Fuego	MB			1					M					B		
[I.2] Daños por agua	MB			1					M					B		
[I.*] Desastres naturales	MB			1					M					B		
[I.3] Contaminación mecánica	MB			1					B					MB		
[I.4] Contaminación electromagnética	MB			1					B					MB		
[I.5] Avería de origen físico o lógico	MB			1					B					MB		
[I.6] Corte de suministro eléctrico	MB			1					M					B		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			1					B					MB		
[I.11] Emanaciones electromagnéticas	MB			1					B					MB		
[E.2] Errores del administrador	B	1	1	1			B	M	MB			B	M	MB		
[E.23] Errores de mantenimiento / actualización de equipos	B			1					B					B		
[E.24] Caída del sistema por agotamiento de recursos	MB			1					B					MB		
[E.25] Perdida de equipos	MB		1	1				B	MB				MB	MB		
[A.6] Abuso de privilegios de acceso	MB	1	10	1			B	A	B			MB	M	MB		
[A.7] Uso no previsto	MB	1	10	1			B	A	B			MB	M	MB		
[A.11] Acceso no autorizado	MB	1	1				B	M				MB	B			
[A.23] Manipulación de los equipos	MB	1	1				B	M				MB	B			
[A.24] Denegación de servicio	MB			10					M					B		
[A.25] Robo	MB		1	10				B	M				MB	B		
[A.26] Ataque destructivo	MB			10					M					B		

Tabla 138. Salvaguardas. Impacto y Riesgo (residual) del activo HW011- Switch

[HW] Hardware		HW011 – Switch														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		A		MA				A		A				
Salvaguardas aplicadas		[SW.A] Copia de seguridad configuración => [D] [H.AC] Ctrl acceso lógico => [A.11], [C] [L.AC] Control acceso físico => [C], [A.7],[A.25] [H.IA] Identificación y autenticación => [C] [HW] Protección Equipos Informáticos => [I]						[HW.A] Aseguramiento disponibilidad => [D], [A.24] [HW.CM] Cambios (actualizaciones y mantenimiento) => [E.23], [E.24], [I.*] [BC] Continuidad del negocio => [E.2] Política de Seguridad CPD Dedicado [I.1], [I.2], [I.3], [I.7], [I.*]							
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			10						A					M		
[I.1] Fuego	MB			10						A					M		
[I.2] Daños por agua	MB			10						A					M		
[I.*] Desastres naturales	MB			10						A					M		
[I.3] Contaminación mecánica	MB			1						M					B		
[I.4] Contaminación electromagnética	MB			1						M					B		
[I.5] Avería de origen físico o lógico	MB			10						A					M		
[I.6] Corte de suministro eléctrico	MB			10						A					M		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			10						A					M		
[I.11] Emanaciones electromagnéticas	MB			1						M					B		
[E.2] Errores del administrador	MB	1	1	1				B	B	M			MB	MB	B		
[E.23] Errores de mantenimiento / actualización de equipos	MB			1						M					B		
[E.24] Caída del sistema por agotamiento de recursos	MB			1						M					B		
[E.25] Perdida de equipos	MB		1	10					B	A				MB	M		
[A.6] Abuso de privilegios de acceso	MB	1	10	1				B	M	M			MB	B	B		
[A.7] Uso no previsto	MB	1	10	1				B	M	M			MB	B	B		
[A.11] Acceso no autorizado	MB	1	10					B	M				MB	B			
[A.23] Manipulación de los equipos	MB	10	1					M	B				B	MB			
[A.24] Denegación de servicio	MB			10						A					M		
[A.25] Robo	MB		1	10					B	A				MB	M		
[A.26] Ataque destructivo	MB			10						A					M		

Tabla 139. Salvaguardas. Impacto y Riesgo (residual) del activo HW014- Mini-switch

[HW] Hardware		HW014 – Mini-switch														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		MA		MA				A		MA				
Salvaguardas aplicadas		[H.AC] Ctrl acceso lógico => [A.11], [C] [L.AC] Control acceso físico => [C], [A.7],[A.25] [H.IA] Identificación y autenticación => [C] [HW] Protección Equipos Informáticos => [I], [I.1], [I.2], [I.5], [E.25]						[HW.A] Aseguramiento disponibilidad => [D], [A.24] [HW.CM] Cambios (actualizaciones y mantenimiento) => [E.23], [E.24], [I.*] Política de Seguridad								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			10						A						M		
[I.1] Fuego	MB			10						A						M		
[I.2] Daños por agua	MB			10						A						M		
[I.*] Desastres naturales	MB			10						A						M		
[I.3] Contaminación mecánica	M			1						M						M		
[I.4] Contaminación electromagnética	B			1						M						M		
[I.5] Avería de origen físico o lógico	MB			10						A						M		
[I.6] Corte de suministro eléctrico	MB			10						A						M		
[I.7] Condiciones inadecuadas de temperatura o humedad	B			1						M						M		
[I.11] Emanaciones electromagnéticas	MB			1						M						B		
[E.2] Errores del administrador	B	1	1	1				B	M	M				B	M	M		
[E.23] Errores de mantenimiento / actualización de equipos	MB			1						M						B		
[E.24] Caída del sistema por agotamiento de recursos	MB			10						A						M		
[E.25] Perdida de equipos	MB		1	10					M	A					M	M		
[A.6] Abuso de privilegios de acceso	MB	1	10	1				B	A	M				MB	M	B		
[A.7] Uso no previsto	MB	1	10	1				B	A	M						M		
[A.11] Acceso no autorizado	MB	1	10					B	A					MB	M			
[A.23] Manipulación de los equipos	MB	10	1					M	M					B	B			
[A.24] Denegación de servicio	B			10						A						M		
[A.25] Robo	MB		1	10					M	A					B	M		
[A.26] Ataque destructivo	MB			10						A						M		

Tabla 140. Salvaguardas. Impacto y Riesgo (residual) del activo HW016- Terminales

[HW] Hardware		HW016 – Terminales														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		B		A				A		A				
Salvaguardas aplicadas		[D.A] Copias de seguridad de los datos => [D] [H.AC] Ctrl acceso lógico => [A.11], [C] [H.AU] Registro, auditoría => [A.6] [HW] Protección Equipos Informáticos => [I]						[HW.CM] Cambios (actualizaciones y mantenimiento) => [E.23], [E.24], [I.*] [BC] Continuidad del negocio => [E.2] Política de Seguridad => [A.7]								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual		
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			10					M					B		
[I.1] Fuego	MB			10					M					B		
[I.2] Daños por agua	B			10					M					M		
[I.*] Desastres naturales	MB			10					M					B		
[I.3] Contaminación mecánica	MB			10					M					B		
[I.4] Contaminación electromagnética	MB			1					B					MB		
[I.5] Avería de origen físico o lógico	MB			10					M					B		
[I.6] Corte de suministro eléctrico	MB			10					M					B		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			1					B					MB		
[I.11] Emanaciones electromagnéticas	MB			1					B					MB		
[E.2] Errores del administrador	MB	1	1	1			B	MB	B			MB	MB	MB		
[E.23] Errores de mantenimiento / actualización de equipos	MB			1					B					MB		
[E.24] Caída del sistema por agotamiento de recursos	MB			1					B					MB		
[E.25] Perdida de equipos	MB		100	1				B	B				MB	MB		
[A.6] Abuso de privilegios de acceso	MB	1	100	1			B	B	B			MB	MB	MB		
[A.7] Uso no previsto	MB	1	10	1			B	MB				MB	MB			
[A.11] Acceso no autorizado	MB	1	10				B	MB				MB	MB			
[A.23] Manipulación de los equipos	MB	1	10				B	MB				MB	MB			
[A.24] Denegación de servicio	MB			10					M					B		
[A.25] Robo	MB		100	10				B	M				MB	B		
[A.26] Ataque destructivo	MB			10					M					B		

Tabla 141. Salvaguardas. Impacto y Riesgo (residual) del activo HW018- Servidor de copias

[HW] Hardware		HW018 – Servidor de copias														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		A		A		A		A		A				
Salvaguardas aplicadas		[H.AC] Ctrl acceso lógico => [C], [A.11] [L.AC] Control acceso físico => [C], [A.25] [D.C] Cifrado de la información => [C]						[HW.A] Aseguramiento de la disponibilidad => [D] Política de Seguridad CPD Dedicado [I.1], [I.2], [I.3], [I.7], [I.*]								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual		
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			10					M					B		
[I.1] Fuego	MB			10					M					B		
[I.2] Daños por agua	MB			10					M					B		
[I.*] Desastres naturales	MB			10					M					B		
[I.3] Contaminación mecánica	MB			1					B					MB		
[I.4] Contaminación electromagnética	MB			1					B					MB		
[I.5] Avería de origen físico o lógico	MB			10					M					B		
[I.6] Corte de suministro eléctrico	MB			10					M					B		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			1					B					MB		
[I.11] Emanaciones electromagnéticas	MB			1					B					MB		
[E.2] Errores del administrador	MB	10	10	1			M	M	B			B	B	MB		
[E.23] Errores de mantenimiento / actualización de equipos	MB			1					B					MB		
[E.24] Caída del sistema por agotamiento de recursos	B			1					B					B		
[E.25] Perdida de equipos	MB		10	10				M	M				B	B		
[A.6] Abuso de privilegios de acceso	B	10	10	1			M	M	B			M	M	B		
[A.7] Uso no previsto	MB	10	10	1			M	M	B			B	B	MB		
[A.11] Acceso no autorizado	MB	10	1				M	B				B	MB			
[A.23] Manipulación de los equipos	MB	10	1				M	B				B	MB			
[A.24] Denegación de servicio	MB			10					M					B		
[A.25] Robo	MB		10	10				M	M				B	B		
[A.26] Ataque destructivo	MB			10					M					B		

7.4.5. [COM] Redes de comunicaciones (impacto y riesgo residual)

Tabla 142. Salvaguardas. Impacto y Riesgo (residual) del activo COM001- Red local LAN

[COM] Redes de comunicaciones		COM001 – Red local LAN														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA		A		A		MA				
Salvaguardas aplicadas		[H.AC] Control de acceso lógico => [A.11] [L.AC] Control de los accesos físicos => [A.11] [H.AU] Registro y auditoría => [A.6], [A.15] [COM.DS] Segregación de las redes en dominios => [C] [COM.SC] Se aplican perfiles de seguridad => [C] [COM.C] Protección criptogr. => [C] [H.tools.CC] Herramienta de chequeo de configuración => [E.2]						[COM.A] Aseguramiento de la disponibilidad => [D], [E.24] [COM.aut] Autenticación del canal => [A] [COM.I] Protección de la integridad de los datos intercambiados => [I] [H.tools.IDS] IDS/IPS: Herramienta de detección / prevención de intrusión => [A.5], [A.7], [A.9] [COM.CM] Cambios (actualizaciones y mantenimiento) => [E.24] Política de Seguridad => Apoyo							
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	MB			10					A					M		
[E.2] Errores del administrador	MB	1	1	1			M	M	M			B	B	B		
[E.9] Errores de re-encaminamiento	MB		10					A					M			
[E.10] Errores de secuencia	MB	1					M					B				
[E.15] Alteración accidental de la información	MB	1					M					B				
[E.18] Destrucción de la información	MB			1					M					B		
[E.19] Fugas de información	MB		1					M					B			
[E.24] Caída del sistema por agotamiento de recursos	MB			10					A					M		
[A.5] Suplantación de la identidad del usuario	MB	1	10		10		M	A		M		B	M		B	
[A.6] Abuso de privilegios de acceso	MB	1	10	1			M	A	M			B	M	B		
[A.7] Uso no previsto	MB	1	10	1			M	A	M			B	M	B		
[A.9] Re-encaminamiento de mensajes	MB		10					A					M			
[A.10] Alteración de secuencia	MB	1					M					B				
[A.11] Acceso no autorizado	MB	1	10				M	A				B	M			
[A.12] Análisis de trafico	MB		10					A					M			
[A.14] Interceptación de información (escucha)	MB		10					A					M			
[A.15] Modificación deliberada de la información	MB	1					M					B				
[A.19] Divulgación de información	M		1					M					M			
[A.24] Denegación de servicio	MB			10					A					M		

Tabla 143. Salvaguardas. Impacto y Riesgo (residual) del activo COM005- Fibra

[COM] Redes de comunicaciones		COM005 – Fibra														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		A		MA		MA		A		A		MA				
Salvaguardas aplicadas		[L.AC] Control de los accesos físicos => [C] [COM.A] Aseguramiento de la disponibilidad => [D], [E.24]						Plan de contingencia => [A.24] Política de Seguridad => Apoyo								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual		
	Frecuencia	[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	MB			10						A					M		
[E.2] Errores del administrador	MB	1	1	1				B	M	M			MB	B	B		
[E.9] Errores de re-encaminamiento	MB		10						A					M			
[E.10] Errores de secuencia	MB	10						M					B				
[E.15] Alteración accidental de la información	MB	1						B					MB				
[E.18] Destrucción de la información	MB			1						M					B		
[E.19] Fugas de información	MB		1						M					B			
[E.24] Caída del sistema por agotamiento de recursos	MB			10						A					M		
[A.5] Suplantación de la identidad del usuario	MB	10	10		100			M	A		A		B	M		M	
[A.6] Abuso de privilegios de acceso	MB	1	10	1				B	A	M			MB	M	B		
[A.7] Uso no previsto	MB	10	10	1				M	A	M			B	M	B		
[A.9] Re-encaminamiento de mensajes	MB		10						A					M			
[A.10] Alteración de secuencia	MB	10						M					B				
[A.11] Acceso no autorizado	MB	1	10					B	A				MB	M			
[A.12] Análisis de trafico	MB		10						A					M			
[A.14] Interceptación de información (escucha)	MB		10						A					M			
[A.15] Modificación deliberada de la información	B	10						M					M				
[A.19] Divulgación de información	M		1						M					M			
[A.24] Denegación de servicio	MB			10						A					M		

7.4.6. [Media] Soportes de información (impacto y riesgo residual)

Tabla 144. Salvaguardas. Impacto y Riesgo (residual) del activo MEDIA001- Discos duros extraíbles

[MEDIA] Soportes de información		MEDIA001 Discos duros extraíbles														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		A						MA				
Salvaguardas aplicadas		[MP] Protección de los Soportes de Info. => [I] y [N], [I.*], [E.25], [A.11], [A.25] [MP.end] Destrucción de soportes						[MP.A] Aseguramiento de la disponibilidad => [D] [MP.IC] Protección criptográfica del contenido => [C] Política de Seguridad => Apoyo								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual		
	Frecuencia	[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			10						M					B		
[I.1] Fuego	MB			10						M					B		
[I.2] Daños por agua	MB			10						M					B		
[I.*] Desastres naturales	MB			10						M					B		
[I.3] Contaminación mecánica	MB			1						B					B		
[I.4] Contaminación electromag.	MB			10						M					B		
[I.5] Avería de origen físico o lógico	MB			10						M					B		
[I.6] Corte de suministro eléctrico	MB			10						M					B		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			1						B					MB		
[I.10] Degradación de los soportes	MB			1						B					MB		
[I.11] Emanaciones electromag.	MB			1						B					MB		
[E.1] Errores de los usuarios	MB	1	10	1				M	A	B			B	M	MB		
[E.2] Errores del administrador	MB	1	10	10				M	A	M			B	M	B		
[E.15] Alteración accidental de info.	MB	1						M					B				
[E.18] Destrucción de la información	MB			10						M					B		
[E.19] Fugas de información	MB		10						A					M			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B			1						B					B		
[E.25] Perdida de equipos	MB		10	10					A	M				M	B		
[A.7] Uso no previsto	MB	10	10	10				A	A	M			M	M	B		
[A.11] Acceso no autorizado	MB	1	1					M	M				B	B			
[A.15] Modificación adrede de info.	MB	10						A					M				
[A.18] Destrucción de la información	MB			10						M					B		
[A.19] Divulgación de información	MB		1						M					B			
[A.23] Manipulación de los equipos	MB		1	1					M	B				B	MB		
[A.25] Robo	MB		10	10					A	M				M	B		
[A.26] Ataque destructivo	MB			10						M					B		

Tabla 145. Salvaguardas. Impacto y Riesgo (residual) del activo MEDIA002- Blue-Ray

[MEDIA] Soportes de información		MEDIA002 Blue-Ray														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		A		B						A				
Salvaguardas aplicadas		[MP] Protección de los Soportes de Info. => [I] y [N], [I.*], [E.19], [E.25], [A.11], [A.25] [MP.end] Destrucción de soportes						[MP.A] Aseguramiento de la disponibilidad => [D] [MP.IC] Protección criptográfica del contenido => [C] Política de Seguridad => Apoyo								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual		
	Frecuencia	[I]	[C]	[D]	[A]	[T]		[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			10						MB					MB		
[I.1] Fuego	MB			10						MB					MB		
[I.2] Daños por agua	MB			10						MB					MB		
[I.*] Desastres naturales	MB			10						MB					MB		
[I.3] Contaminación mecánica	MB			10						MB					MB		
[I.4] Contaminación electromag.	MB			10						MB					MB		
[I.5] Avería de origen físico o lógico	MB			10						MB					MB		
[I.6] Corte de suministro eléctrico	MB			10						MB					MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			10						MB					MB		
[I.10] Degradación de los soportes	MB			1						MB					MB		
[I.11] Emanaciones electromag.	MB			1						MB					MB		
[E.1] Errores de los usuarios	MB	1	10	1				B	M	MB			MB	B	MB		
[E.2] Errores del administrador	MB	1	10	10				B	M	MB			MB	B	MB		
[E.15] Alteración accidental de info.	MB	10						B					MB				
[E.18] Destrucción de la información	MB			10						MB					MB		
[E.19] Fugas de información	MB		10						M					B			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MB			1						MB					MB		
[E.25] Perdida de equipos	MB		10	10					M	MB				B	MB		
[A.7] Uso no previsto	MB	10	10	10				B	M	MB			MB	B	MB		
[A.11] Acceso no autorizado	MB	1	10					B	M				MB	B			
[A.15] Modificación adrede de info.	MB	10						B					MB				
[A.18] Destrucción de la información	MB			10						MB					MB		
[A.19] Divulgación de información	MB		10						M					B			
[A.23] Manipulación de los equipos	MB		1	1					B	MB				MB	MB		
[A.25] Robo	MB		10	10					M	MB				B	MB		
[A.26] Ataque destructivo	MB			10						MB					MB		

7.4.7. [L] Instalaciones (impacto y riesgo residual)

Tabla 146. Salvaguardas. Impacto y Riesgo (residual) del activo L001- Nave principal

[L] Instalaciones		L001 Nave principal														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA						MA				
Salvaguardas aplicadas		[L] Protección de las Instalaciones => [C], [D] [L.AC] Control de los accesos físicos => [E.18], [E.19], [A.11]						Política de Seguridad => Apoyo Registro incidentes de seguridad => Apoyo								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual		
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			10					A					M		
[I.1] Fuego	MB			10					A					M		
[I.2] Daños por agua	B			1					M					M		
[I.*] Desastres naturales	MB			1					M					B		
[I.11] Emanaciones electromagnetica	MB			1					M					B		
[E.15] Alteración accidental	MB	100					MA					A				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	B		1					M					M			
[A.7] Uso no previsto	MB	10	1	1			A	M	M			M	B	B		
[A.11] Acceso no autorizado	MB	10	10				A	A				M	M			
[A.15] Modificación deliberada	MB	100					MA					A				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		10					A					M			
[A.26] Ataque destructivo	MB			10					A					M		
[A.27] Ocupación enemiga	MB		10	10				MA	A				A	M		

Tabla 147. Salvaguardas. Impacto y Riesgo (residual) del activo L005- CPD

[L] Instalaciones		L005 CPD														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA						MA				
Salvaguardas aplicadas		[L] Protección de las Instalaciones => [C], [D] [L.AC] Control de los accesos físicos => [E.18], [E.19], [A.11] [AUX.AC] Climatización => [I.1], [I.2]						[AUX.wires] Protección del cableado => [I.1] Política de Seguridad => Apoyo Registro incidentes de seguridad => Apoyo								
Amenazas	Probabilidad residual	Degradación residual						Impacto residual						Riesgo residual		
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[N] Desastres naturales	MB			10					A					M		
[I.1] Fuego	MB			10					A					M		
[I.2] Daños por agua	MB			1					M					B		
[I.*] Desastres naturales	MB			1					M					B		
[I.11] Emanaciones electromagnetica	MB			1					M					B		
[E.15] Alteración accidental	MB	10					A					M				
[E.18] Destrucción de la información	MB			10					A					M		
[E.19] Fugas de información	MB		1					M					B			
[A.7] Uso no previsto	B	10	1	1			A	M	M			M	B	B		
[A.11] Acceso no autorizado	MB	10	10				A	A				M	M			
[A.15] Modificación deliberada	MB	10					A					M				
[A.18] Destrucción de la información	MB			10					A					M		
[A.19] Divulgación de información	MB		10					A					M			
[A.26] Ataque destructivo	MB			10					A					M		
[A.27] Ocupación enemiga	MB		10	10				A	A				A	M		

7.4.8. [P] Personal (impacto y riesgo residual)

Tabla 148. Salvaguardas. Impacto y Riesgo (residual) del activo P001- Gerencia

[P] Personal		P001 Gerencia														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		MA		MA		MA						MA				
Salvaguardas aplicadas		[PS.AT] Formación y concienciación => [C] [PS.A] Aseguramiento de la disponibilidad => [D]						Política de Seguridad => Apoyo Plan de contingencia								
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.19] Fugas de información	MB		10					A					M			
[E.28] Indisponibilidad del personal	MB			10					A					M		
[A.28] Indisponibilidad del personal	MB			10					A					M		
[A.29] Extorsión	MB	100	10	10			A	A	A			M	B	B		
[A.30] Ingeniería social (picaresca)	MB	100	10	10			M	A	A			B	M	M		

Tabla 149. Salvaguardas. Impacto y Riesgo (residual) del activo P002- Oficina

[P] Personal		P002 Oficina														
Valor		[I]		[C]		[D]		[A]		[T]		TOTAL				
		M		MA		M						MA				
Salvaguardas aplicadas		[PS.AT] Formación y concienciación => [C] [PS.A] Aseguramiento de la disponibilidad => [D]						Política de Seguridad => Apoyo Elaboración de procedimientos								
Amenazas	Probabilidad residual	Degradación residual					Impacto residual					Riesgo residual				
	Frecuencia	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]	[I]	[C]	[D]	[A]	[T]
[E.19] Fugas de información	MB		10					M					B			
[E.28] Indisponibilidad del personal	MB			10					B					MB		
[A.28] Indisponibilidad del personal	MB			1					MB					MB		
[A.29] Extorsión	MB	10	10	1			B	A	MB			MB	M	MB		
[A.30] Ingeniería social (picaresca)	MB	10	10	10			B	A	B			MB	M	MB		

8. Identificación de los proyectos de seguridad

El análisis de la aplicación de salvaguardas sobre los activos nos ha proporcionado una idea aproximada de la reducción en el impacto y probabilidad, y por tanto el riesgo, que la instalación de las salvaguardas conllevara. Por lo tanto, a continuación, analizaremos las salvaguardas para seleccionar de entre todas, aquellas que su aplicación implicará un mayor descenso del impacto/probabilidad y a su vez tengan una buena relación coste/beneficio, buscando un equilibrio entre la inversión económica/temporal y el beneficio que generará para la empresa.

Tras la selección de salvaguardas, realizaremos la agrupación de las más relacionadas entre sí (complementarias o afines), con el objetivo de generar los planes de seguridad para proteger los activos más valiosos del grupo empresarial. Finalmente, estos planes los acabaremos empleando en establecer la estrategia de implantación global del sistema de gestión de seguridad de la información corporativo, el conocido como Plan Director de Seguridad.

8.1. Tratamiento del riesgo

Una vez realizado el análisis de impacto/probabilidad de los activos, sus riesgos y su impacto/probabilidad residual tras la aplicación de las salvaguardas, se realizará la evaluación y tratamiento de los riesgos para determinar la decisión y acción (aceptación, eliminación, mitigación o compartición) que la dirección de la organización realizará sobre los riesgos. Esta evaluación y tratamiento, se realizará empleando como base las tablas del cálculo de impacto y riesgo residual tras la aplicación de las salvaguardas generadas en el apartado anterior.

La dirección ha determinado emplear los umbrales de riesgo de los activos con el objetivo de establecer un criterio general para decidir cuales riesgos serán asumidos por la empresa y cuales requerirán tratamiento. Por lo tanto, se aplicará el siguiente criterio de tratamiento:

- **Activos con una estimación de riesgo bajo (B) o muy bajo (MB):** la materialización de amenazas es muy improbable o el impacto apenas es apreciable. Por lo tanto, la postura de la organización ante el riesgo sobre estos activos es la **ACEPTACIÓN**.
- **Activos con una estimación de riesgo medio (M):** en estos casos la organización ha decidido que su protección no tiene prioridad, por lo que se delegará la mitigación de estos riesgos a los planes de concienciación, formación y los planes de contingencia. Se trata de una postura de **ACEPTACIÓN**.

- **Activos con una estimación de riesgo alto (A) o muy alto (MA):** la probabilidad de materialización de amenazas es muy alta o su daño será crítico para la empresa. Por lo tanto, la postura de la organización ante el riesgo sobre estos activos es el de tratar de reducirlos empleando salvaguardas hasta reducir el riesgo a un nivel asumible, **MITIGACIÓN o COMPARTICIÓN**.

Por otra parte, es importante destacar que la mayor parte de los activos sobre los que no se han realizado análisis de impacto y riesgo, son activos que se encuentran compartidos con otras empresas, como lo es el caso de S002 - Portal Web de la empresa, HW008 – Impresoras, COM002 – ADSL, COM003 - Servicio telefonía, COM006 – Fibra oscura. Estos casos el tratamiento del riesgo es COMPARTIDO

A continuación, se detalla el análisis de salvaguardas a aplicar de forma activa sobre los activos.

8.1.1. [D] Datos / Información (tratamiento del riesgo)

- **D001 – Documentación y planos, D002 – Archivo clientes, D010 – Datos personal empresa**

Estos archivos se refieren a la información relacionada con la documentación y planos de los productos que la empresa fabrica, la información acerca de los clientes con los que el grupo empresarial trabaja y los datos acerca del personal interno de la empresa. La mayor parte de esta información es crítica para el funcionamiento de la empresa y de carácter sensible, lo tanto es indispensable asegurar su completa protección.

En estos activos, las **amenazas** que provocan los mayores riesgos son: *[E.1] Errores de los usuarios, [E.15] Alteración accidental de la información, [E.18] Destrucción de la información, [E.19] Fugas de información, [A.5] Suplantación de la identidad del usuario, [A.6] Abuso de privilegios de acceso, [A.11] Acceso no autorizado, [A.15] Modificación deliberada de la información, [A.18] Destrucción de la información, [A.19] Divulgación de información.*

La gran mayoría de estas amenazas corresponden al acceso indebido a los ficheros y a la no existencia de una auditoria que pueda reflejar los cambios realizados en los ficheros por los empleados.

Por lo tanto, las **salvaguardas** que se contemplan son: [H.AU] Registro, auditoría, [H.AC] Control de acceso lógico, [H.IA] Identificación, autenticación, [D.C] Cifrado información, [D.A] Copias de

seguridad de los datos (backup), [D.I] Aseguramiento integridad, [PS.AT] Formación y concienciación, Política de Seguridad.

- *[H.AU] Registro, auditoría*: Se establecerá un nivel de auditoria y registro de eventos de seguridad relacionados con el acceso y modificación de los activos más críticos y sensibles. Se deberán registrar los datos de los usuarios con su fecha y hora del evento sobre: accesos correctos e incorrectos, creaciones, modificaciones (información y permisos).

- *[H.AC] Control de acceso lógico, [H.IA] Identificación, autenticación*: Se establecerán una serie de permisos para asegurar que solo sean accesibles por el personal responsable, asegurando así su confidencialidad y autenticidad.

- *[D.C] Cifrado información*: dependiendo de la sensibilidad de la información, la información más sensible se deberá de cifrar para impedir riesgos en la confidencialidad. Este aspecto se reflejará en la política de seguridad.

- *[D.A] Copias de seguridad de los datos (backup)*: al realizar copias de estos archivos se puede asegurar la disponibilidad de estos activos de la información ante cualquier incidencia. En la política de copias de seguridad se deberá de definir el nivel de criticidad y los intervalos entre copia y copia para estos activos.

- *[D.I] Aseguramiento integridad*: Para proteger la integridad de los archivos más cruciales se realizara un cálculo de los hash, detectando así con el cambio del hash cualquier cambio no registrado en estos ficheros.

- *[PS.AT] Formación y concienciación*: la formación y concienciación en materia de seguridad es indispensable para proteger la confidencialidad, ayudando a disminuir los riesgos de todas las amenazas referentes a las posibles las fugas o divulgaciones de información. Además, es necesario dar a conocer que para estos ficheros es necesario cumplir con la Ley Orgánica de Protección de Datos (LOPD) [3].

- *Política de Seguridad*: en la política de seguridad de la información se deben definir las políticas con la normativa interna en materia de seguridad de la información que garanticen que la LOPD se cumpla. Se deben de reflejar aspectos como los usuarios que pueden acceder a los ficheros, el nivel de permisos, la auditoria sobre los datos, la política de copias, etc.

- **D005 – Copias de seguridad**

Las copias de seguridad de los datos del servidor presentan información muy sensible y critica, por lo que es necesaria su protección. Actualmente, ya está siendo protegida empleando diversas salvaguardas por lo que ya presenta resistencia a gran parte de las amenazas.

Las **amenazas** que presentan los mayores riesgos en este activo son: *[E.2] Errores del administrador, [E.18] Destrucción de la información, [A.18] Destrucción de la información*.

Las medidas que se podrán adoptar intentarán comprobar la integridad de las copias y asegurar la disponibilidad.

Por lo tanto, las **salvaguardas** que se contemplan son: *[H.AC] Ctrl acceso lógico, [D.C] Cifrado información, [BC] Continuidad del negocio, Política de Seguridad*.

- *[H.AC] Control de acceso lógico*: Esta salvaguarda actualmente ya se encuentra aplicada, establece medidas de seguridad para el acceso a las copias.

- *[D.C] Cifrado de la información*: Esta salvaguarda actualmente ya se encuentra aplicada, realiza una encriptación de las copias de seguridad.

- *[BC] Continuidad de negocio*: En el plan de contingencia se establecerá una serie de comprobaciones periódicas planificadas y contempladas en la política de seguridad corporativa, con el objetivo de comprobar la validez de las copias.

Además, se buscará la forma de poder guardar las copias de seguridad en una localización segura y externa a las localizaciones del grupo empresarial, como un sistema de almacenamiento en la nube.

- *Política de seguridad*: Actualmente las copias se realizan de una forma completamente informal, por lo que será necesario establecer una política de copias de seguridad dentro de la política de seguridad. La política de copias de seguridad establecerá la información sobre la que se debe realizar copias, cada cuanto intervalo de tiempo se realizara, cuando se realizaran comprobaciones de la validez de estas, el tiempo máximo de preservación de las copias y se establecerá una configuración de logs que permita revisar el estado de las copias y analizar posibles errores.

- **D006 – Ficheros de LOG, D007 – Ficheros de configuración**

Estos activos refieren a los archivos de LOG y de configuraciones, ambos presentan riesgos elevados que deben ser mitigados.

En estos activos, las **amenazas** que provocan los mayores riesgos son: [E.2] Errores del administrador, [E.18] Destrucción de la información, [A.11] Acceso no autorizado, [A.15] Modificación deliberada de la información, [A.18] Destrucción de la información, [A.19] Divulgación de información.

Como puede observarse, la mayor parte de las amenazas corresponden al acceso indebido a estos ficheros, por lo que la prioridad de las salvaguardas será la de evitar los accesos no autorizados a los logs y las configuraciones.

Por lo tanto, las **salvaguardas** que se contemplan son: *[H.AU] Registro, auditoría, [H.AC] Control del acceso lógico, [H.IA] Identificación autenticación, [H.tools.CC] Herramienta de chequeo de configuración, [H.tools.LA] Herramienta análisis logs, [D.A] Copias de seguridad de los datos (backup), [D.I] Aseguramiento integridad, Política de Seguridad*.

- *[H.AU] Registro, auditoría*: Se establecerá un nivel de auditoria suficiente para asegurar la trazabilidad y el no repudio. En los archivos de configuración se realizara un registro de accesos y de modificaciones.

- *[H.AC] Control del acceso lógico*, *[H.IA] Identificación autenticación*: Se establecerán una serie de permisos para asegurar que solo sean accesibles por el personal responsable, asegurando así su confidencialidad y autenticidad.

- *[H.tools.CC] Herramienta de chequeo de configuración*: esta herramienta ayudará a que el administrador evite errores en las configuraciones de las aplicaciones.

- *[H.tools.LA] Herramienta análisis logs:* Actualmente los logs apenas carecen de valor y solamente se utilizan cuando algo deja de funcionar o se quiere comprobar algún comportamiento en concreto. Por lo que una herramienta de análisis de logs ayudaría en la gestión y análisis de los eventos de logs y monitorización de los sistemas. La información de los logs es crucial para realizar el análisis de incidentes, determinar la extensión de un ataque o depurar responsabilidades.

- *[D.A] Copias de seguridad de los datos (backup):* realizando copias de seguridad de las configuraciones y los logs se puede evitar la destrucción de la información, así como una pronta recuperación en el caso de se pierdan.

- *[D.I] Aseguramiento integridad:* Para proteger la integridad de los archivos de configuración se realizara un cálculo de los hash, detectando así con el cambio del hash cualquier cambio en estos.

- *Política de Seguridad:* en la política de seguridad corporativa se debe reflejar las configuraciones y logs sensibles a proteger, las características de las copias de seguridad que se realicen de estos (intervalos, total/incremental…), así como la información que se debe recoger en los logs a nivel de auditoria.

- **D008 - Base de datos del ERP, D009 - Base de datos del gestor de proyectos**

Estos archivos se refieren a las bases de datos donde se almacenan los datos de las producciones y proyectos del grupo empresarial. La mayor parte de esta información es crítica para el funcionamiento de la empresa, lo tanto es indispensable asegurar su disponibilidad y confidencialidad.

En estos activos, las **amenazas** que provocan los mayores riesgos son: *[E.2] Errores del administrador, [E.18] Destrucción de la información, [A.15] Modificación deliberada de la información, [A.18] Destrucción de la información, [A.19] Divulgación de información.*

La gran mayoría de estas amenazas corresponden al acceso indebido a las bases de datos y a la posibilidad de que puedan ocurrir incidentes con la gestión de las bases de datos, que las dejen funcionando con errores o no usables, ya que muchas veces al no disponer de un entorno de pruebas controlado se realizan modificaciones directamente sobre las bases de datos de producción, suponiendo un gran riesgo en la disponibilidad.

Por lo tanto, las **salvaguardas** que se contemplan son: *[H.AU] Registro, auditoría, [H.AC] Control de acceso lógico, [H.IA] Identificación, autenticación, [D.C] Cifrado información, [D.A] Copias de seguridad de los datos (backup), [D.I] Aseguramiento integridad, [BC] Continuidad del negocio, Política de Seguridad*.

- [H.AU] Registro, auditoría: Se establecerá un nivel de auditoria y registro de eventos de seguridad relacionados con el acceso y modificación. Será necesario registrar las conexiones realizadas, ya sean correctas o incorrectas, junto con las acciones de creación, modificación y eliminación de datos que aseguren el no repudio.

- [H.AC] Control del acceso lógico, [H.IA] Identificación autenticación: Se establecerán una serie de permisos y usuarios para asegurar que solo sean accesibles por el personal responsable, asegurando así su confidencialidad y autenticidad.

- *[D.C] Cifrado información*: dependiendo de la sensibilidad de la información, la información más sensible se deberá de cifrar para impedir riesgos en la confidencialidad. Este aspecto se reflejará en la política de seguridad.

- [D.A] Copias de seguridad de los datos (backup): realizando copias de seguridad de las bases de datos se puede evitar la destrucción de la información, así como una pronta recuperación en el caso de se pierdan.

- [D.I] Aseguramiento integridad: Para proteger la integridad de las bases de datos se realizaran comprobaciones de forma periódica que aseguren que no se hayan producido ataques a la integridad de estas.

- [BC] Continuidad de negocio: en el plan de continuidad se debe registrar las acciones a seguir en el caso de que se produzca un incidente que deje inservible la base de datos, así como la recuperación pronta de una copia de seguridad y la recuperación de los datos entre la última copia de seguridad y el incidente.

- Política de Seguridad: en la política de seguridad corporativa se deben reflejar las configuraciones de las bases de datos, la información que se debe de proteger, las características de las copias de seguridad que se realicen de estos (intervalos, total/incremental…), así como la jerarquía de permisos que existen en estas bases de datos.

8.1.2. [S] Servicios (tratamiento del riesgo)

- **S003 – VPN**

Este activo se refiere al servicio VPN que actualmente es usado por los trabajadores en remoto y por los empleados del departamento de informática cuando requieren conectarse a la LAN desde una localización externa a la empresa.

En estos activos, las **amenazas** que provocan los mayores riesgos son: *[E.9] Errores de re-encaminamiento, [A.5] Suplantación identidad, [A.9] Re-encaminamiento mensajes, [A.11] Acceso no autorizado, [A.19] Divulgación de información.*

La gran mayoría de estas amenazas corresponden al acceso no autorizado al uso del servicio VPN. Un acceso no autorizado al servicio de VPN podría suponer una brecha de seguridad que afectaría en su mayor parte a la dimensión de confidencialidad.

Por lo tanto, las **salvaguardas** que se contemplan son: [H.AU] Registro, auditoría, [H.AC] Control acceso lógico, [H.IA] Identificación, autenticación, [S.A] Aseguramiento de la disponibilidad, [S.SC] Se aplican perfiles de seguridad, [BC] Continuidad del negocio, [H.tools.TM] Herramienta de monitorización de tráfico, Política de Seguridad.

- *[H.AU] Registro, auditoría*: Se establecerá un nivel de auditoria suficiente para asegurar la trazabilidad de las conexiones realizadas y el no repudio. Con ello se podrá reforzar el servicio ante la amenaza de divulgación de información.

- *[H.AC] Control acceso lógico, [H.IA] Identificación, autenticación*: Se establecerá el acceso mediante el uso de certificados, para evitar el uso de usuario y contraseña que se viene realizando hoy en día. Con ello se evitará el riesgo de accesos no autorizados y suplantación de identidad.

- *[S.A] Aseguramiento de la disponibilidad*: es imperativo configurar el servicio de tal forma, que cuando caiga, vuelva a iniciarse y avise a los administradores del sistema, por si requiere la acción del administrador.

- *[S.SC] Se aplican perfiles de seguridad*: Aplicando unos perfiles de seguridad se puede controlar las acciones permitidas a los usuarios, con lo que se puede evitar accesos no autorizados.

- *[BC] Continuidad del negocio*: en el plan de continuidad se debe registrar las acciones a seguir para volver a levantar el servicio en el caso de que se produzca un incidente que deje la VPN inutilizada y no funcione la automatización que lo levante automáticamente.

- *[H.tools.TM] Herramienta de monitorización de tráfico*: con una herramienta de monitorización de las conexiones se puede controlar que usuarios están empleando la VPN en cada momento, para detectar conexiones incorrectas o sospechosas que puedan llevar a accesos no autorizados o divulgación de información.

- *Política de Seguridad*: en la política de seguridad corporativa se deben reflejar las configuraciones de la VPN, los usuarios que tienen permiso para emplear el servicio, las normas sobre el uso de la VPN y sus riesgos (no permitiendo a gente externa el uso de los certificados de acceso, por ejemplo).

- **S004 – Virtualización servidores**

Estos activos refieren al servicio de virtualización de servidores que permite disponer de instancias de servidores virtuales empleando solamente una máquina servidora. Este servicio

actualmente ya cuenta con ciertas protecciones, por lo que las amenazas que presenta son muy reducidas.

En estos activos, las **amenazas** que provocan los mayores riesgos son: *[E.2] Errores del administrador, [A.13] Repudio.*

La gran mayoría de estas amenazas corresponden a errores que podría cometer la administración del servicio con la configuración de las instancias.

Por lo tanto, las **salvaguardas** que se contemplan son: *[H.AU] Registro, auditoría, [BC] Continuidad del negocio, Política de Seguridad.* Se han decidido descartar las salvaguardas que ya se encuentran aplicadas, que son: *[H.AC] Control acceso lógico [H.IA] Identificación, autenticación, [S.A] Aseguramiento de la disponibilidad, [S.SC] Se aplican perfiles de seguridad.*

- *[H.AU] Registro, auditoría:* Se establecerá un nivel de auditoria suficiente para asegurar la trazabilidad de las conexiones realizadas y el no repudio. Con ello se podrá reforzar el servicio ante la amenaza no repudio y la depuración de responsabilidades.

- *[BC] Continuidad del negocio:* en el plan de continuidad se debe registrar las acciones a seguir en el caso de que una instancia caiga y sea necesario volver a levantarla.

- *Política de Seguridad:* en la política de seguridad corporativa se deben reflejar las instancias disponibles, así como su funcionalidad e información contenida en cada una de ellas.

- **S007 – DNS, S009 – Active Directory, S010 – GPO**

Estos activos se refieren al servicio de Sistema de nombres de dominio (DNS), al servicio de Active Directory y el servicio de Directivas de grupo (GPO). Estos servicios permiten autentificar y autorizar a los usuarios, establecer políticas de grupos y permitir la resolución de nombres de dominio en el interior del grupo empresarial.

En estos activos, las **amenazas** que provocan los mayores riesgos son: *[E.2] Errores del administrador, [A.18] Destrucción de la información, [A.24] Denegación de servicio*

La gran mayoría de estas amenazas corresponden a posibles errores en la configuración de los servicios o amenazas internas que puedan afectar a la disponibilidad de los servicios.

Por lo tanto, las **salvaguardas** que se contemplan son: [H.AU] Registro, auditoría, *[S.A] Aseguramiento de la disponibilidad, [S.dir] Protección del directorio, [S.dns] Protección del servidor DNS, [BC] Continuidad del negocio, Política de Seguridad.* Actualmente, ya se cuentan

con algunas de estas salvaguardas instaladas: *[H.AC] Control acceso lógico, [H.IA] Identificación, autenticación, [S.SC] Se aplican perfiles de seguridad.*

- *[H.AU] Registro, auditoría*: Se establecerá un nivel de auditoria suficiente para asegurar la trazabilidad de las conexiones realizadas y el no repudio.

- *[S.A] Aseguramiento de la disponibilidad*: es imperativo configurar el servicio de tal forma, que cuando caiga, vuelva a iniciarse y avise a los administradores del sistema, por si requiere la acción del administrador. Esto permitiría reforzar los servicios ante la amenaza de denegación del servicio.

- *[S.dir] Protección del directorio*: Al proteger los directorios donde se encuentran estos servicios, se puede evitar la amenaza de destrucción de la información.

- *[S.dns] Protección del servidor DNS*: Se realizarán copias de las configuraciones del DNS para evitar manipulaciones y poder restaurar las configuraciones en caso de necesidad.

- *[BC] Continuidad del negocio*: Se puede estudiar la posibilidad de mantener copias de las configuraciones, para en caso de un incidente, ante la infección o degradación de este, poder restaurarlo o regenerarlo a partir de la copia.

- *Política de Seguridad*: Las características, configuraciones, permisos de acceso y administración deben estar contempladas en la política de seguridad.

- **S015 – Servidor ERP**

En el servicio que ofrece el ERP, las **amenazas** que provocan los mayores riesgos son: *[E.2] Errores del administrador, [A.5] Suplantación de la identidad del usuario, [A.18] Destrucción de la información, [A.24] Denegación de servicio*.

La gran mayoría de estas amenazas corresponden con accesos no autorizados y fallos en la configuración del servicio.

Por lo tanto, las **salvaguardas** que se contemplan son: [H.AU] Registro, auditoría, *[H.AC] Control acceso lógico [H.IA] Identificación, autenticación, [S.A] Aseguramiento de la disponibilidad, [S.SC] Se aplican perfiles de seguridad, [BC] Continuidad del negocio, [S.CM] Gestión de cambios, Política de Seguridad.*

- *[H.AU] Registro, auditoría*: Se establecerá un nivel de auditoria y registro de eventos de seguridad relacionados con el acceso al servicio ERP. Se deberán registrar los datos de los usuarios con su fecha y hora del evento sobre: accesos correctos e incorrectos.

- *[H.AC] Control acceso lógico, [H.IA] Identificación, autenticación*: es necesario establecer un sistema de permisos para limitar los usuarios que se puedan conectar al servicio, limitándolo solo al personal autorizado para ello.

- *[S.A] Aseguramiento de la disponibilidad*: añadir una salvaguarda para asegurar el servicio este siempre disponible permitirá mitigar la amenaza de denegación de servicio.

- *[S.SC] Se aplican perfiles de seguridad*: aplicar perfiles de seguridad permitirá mantener bajo control las acciones que se puedan realizar sobre el servicio ERP

- *[BC] Continuidad del negocio*: en el plan de continuidad se debe registrar las acciones a seguir en el caso de que el servicio caiga y sea necesario volver a levantarlo con todos los pasos a contemplar. También se recomienda incluir un plan de instalación desde cero del servicio y recuperación de los datos del ERP empleando copias de seguridad.

- *[S.CM] Gestión de cambios:* llevar un registro de los cambios realizados en los servicios del ERP permitirá tener una trazabilidad de los eventos y mitigará la posibilidad de que el administrador realice cambios erróneos sobre el servicio.

- *Política de Seguridad*: Las características, configuraciones, permisos de acceso y administración deben estar contempladas en la política de seguridad.

- **S016 – PostgreSQL, S017 – Microsoft SqlServer**

Estos archivos se refieren a las bases de datos que se emplean para almacenar los datos de las aplicaciones del ERP, de las aplicaciones propias de la empresa y del gestor de proyectos. Al tratarse de información crítica para la empresa, la seguridad es imperativa.

En estos activos, las **amenazas** que provocan los mayores riesgos son: *[E.2] Errores del administrador, [E.15] Alteración accidental de la información, [E.18] Destrucción de la información, [E.24] Caída del sistema por agotamiento de recursos, [A.5] Suplantación de la identidad del usuario, [A.10] Alteración de secuencia, [A.11] Acceso no autorizado, [A.13] Repudio, [A.15] Modificación deliberada de la información, [A.18] Destrucción de la información, [A.24] Denegación de servicio.*

La gran mayoría de estas amenazas corresponden a posibles accesos no autorizados, errores en las configuraciones de las bases de datos y modificaciones o borrados indebidos de los datos.

Por lo tanto, las **salvaguardas** que se contemplan son: [H.AU] Registro, auditoría, *[H.AC] Control acceso lógico [H.IA] Identificación, autenticación, [S.A] Aseguramiento de la disponibilidad, [S.SC]*

Se aplican perfiles de seguridad, [BC] Continuidad del negocio, [S.CM] Gestión de cambios, Política de Seguridad.

- *[H.AU] Registro, auditoría*: Se establecerá un nivel de auditoria y registro de eventos de seguridad relacionados con el acceso a los servicios de base de datos. Se deberán registrar los datos de los usuarios con su fecha y hora del evento sobre: accesos correctos e incorrectos, cambios en la configuración y transacciones realizadas.

- *[H.AC] Control acceso lógico, [H.IA] Identificación, autenticación*: es necesario revisar de forma periódica el sistema de permisos para limitar las acciones que los usuarios puedan realizar, eliminar usuarios en desuso...

- *[S.A] Aseguramiento de la disponibilidad*: añadir una salvaguarda para asegurar el servicio este siempre disponible permitirá mitigar la amenaza de denegación de servicio o caídas inesperadas del servicio.

- *[S.SC] Se aplican perfiles de seguridad*: a día de hoy existen perfiles de seguridad, pero sería necesario revisar y documentar los permisos de estos perfiles, ya que a día de hoy se encuentran implementados de un modo informal.

- *[BC] Continuidad del negocio*: en el plan de continuidad se debe registrar las acciones a seguir en el caso de que el servicio de base de datos caiga y sea necesario volver a levantarlo con todos los pasos a contemplar (restaurar copia de seguridad, recuperar datos, etc.).

- *[S.CM] Gestión de cambios:* llevar un registro de los cambios realizados en los servicios de base de datos permitirá tener una trazabilidad de los eventos y mitigará la posibilidad de que el administrador realice cambios erróneos sobre el servicio.

- *Política de Seguridad*: en la política de seguridad de la organización se deben de contemplar las características, configuraciones, permisos de acceso y administración sobre las bases de datos.

8.1.3. [SW] Software (tratamiento del riesgo)

- **SW002 – Cliente de correo**

Para la aplicación que hace la función de correo en el grupo empresarial, las **amenazas** que provocan los mayores riesgos (afectando especialmente a las dimensiones de disponibilidad y confidencialidad) son: *[E.1] Errores de los usuarios, [E.2] Errores del administrador, [E.8] Difusión*

de software dañino, [E.19] Fugas de información, [E.20] Vulnerabilidades de los programas (software), [A.5] Suplantación de la identidad del usuario, [A.7] Uso no previsto, [A.11] Acceso no autorizado, [A.15] Modificación deliberada de la información, [A.18] Destrucción de la información, [A.19] Divulgación de información, [A.22] Manipulación de los programas

La mayor parte de los riesgos tiene relación con el uso incorrecto del cliente de correo y la posibilidad de divulgación, robo y pérdida de información.

Las **salvaguardas** consideradas para mitigar el riesgo que estas amenazas provocan son: *[H.AC] Control del acceso lógico, [SW] Protección de las Aplicaciones Informáticas, [SW.SC] Se aplican perfiles de seguridad, [SW.A] Copias de seguridad (backup), [SW.CM] Cambios (actualizaciones y mantenimiento), [H.tools.AV] Herramienta contra código dañino, [BC] Continuidad del negocio, Política de Seguridad.*

- *[H.AC] Control del acceso lógico, [H.tools.AV] Herramienta contra código dañino:* con estas salvaguardas se reducirán los riesgos relacionados con la difusión de software dañino.

- *[SW] Protección de las Aplicaciones Informáticas: para proteger el cliente de correo ante la manipulación de las configuraciones y la configuración o uso incorrecto de la aplicación.*

- *[SW.SC] Se aplican perfiles de seguridad:* s*e utilizarán los perfiles de usuario de red para asignar políticas de uso relacionadas con el uso del cliente de correo por los empleados (por ejemplo, restringir el envío masivo de correos o el reenvió de información).*

- *[SW.A] Copias de seguridad (backup):* actualmente ya se realizan copias semanales de los correos, pero cabe la posibilidad de ajustar los intervalos para que se realicen más a menudo en los perfiles más críticos.

- *[SW.CM] Cambios (actualizaciones y mantenimiento): es necesario establecer una política de actualizaciones para* mejorar la estabilidad, evitar accesos no autorizados, evitar *errores de software y solucionar aquellas vulnerabilidades que se vayan produciendo y solventando por parte del fabricante del software.*

- *[BC] Continuidad del negocio: en los planes de continuidad de negocio se deben de establecer planes de recuperación de correos electrónicos, restablecimiento del sistema de correo tras detectarse el envío interno de correos con software malicioso que provoque la aparición de los correos de la empresa en una lista negra.*

- *Política de Seguridad: en la política de seguridad deberán quedar reflejadas las normas de uso acerca del correo electrónico (como establecer un uso estrictamente profesional) y sus riesgos.*

- **SW005 – ERP**

Para el software ERP del que se dispone en el grupo empresarial, las **amenazas** que provocan los mayores riesgos son: *[I.5] Avería de origen físico o lógico, [E.1] Errores de los usuarios, [E.2] Errores del administrador, [E.8] Difusión de software dañino, [E.15] Alteración accidental de la información, [E.18] Destrucción de la información, [E.19] Fugas de información, [E.20] Vulnerabilidades de los programas (software), [E.21] Errores de mantenimiento / actualización de programas, [A.5] Suplantación de la identidad del usuario, [A.6] Abuso de privilegios de acceso, [A.7] Uso no previsto, [A.8] Difusión de software dañino, [A.11] Acceso no autorizado, [A.15] Modificación deliberada de la información, [A.19] Divulgación de información, [A.22] Manipulación de los programas*.

Esta aplicación presenta gran cantidad de riesgos, ya que se trata del software que trabaja más información sensible y critica para el buen desarrollo de la labor del grupo empresarial. Por lo tanto, es necesario tratar de reforzar en todo lo posible la seguridad para fortalecerla de accesos no deseados, manipulaciones, filtraciones de información y evitar en todo lo posible que los empleados cometan errores reforzando los conocimientos sobre el uso correcto del software.

Las **salvaguardas** consideradas para mitigar el riesgo que estas amenazas provocan son: *[H.AU] Registro, Auditoria*, *[H.AC] Control del acceso lógico, [SW] Protección de las Aplicaciones Informáticas, [SW.SC] Se aplican perfiles de seguridad, [SW.A] Copias de seguridad (backup), [SW.CM] Cambios (actualizaciones y mantenimiento), [H.tools.LA] Herramienta análisis logs, Manuales y Procedimientos, [PS.AT] Formación y concienciación, Política de Seguridad.*

- *[H.AU] Registro, Auditoria:* Se establecerá un nivel de auditoria y registro de eventos de seguridad relacionados con los accesos de los empleados. Se deberán registrar los datos de los usuarios con su fecha y hora del evento sobre: accesos correctos e incorrectos, manipulación de la información y transacciones realizadas

- *[H.AC] Control del acceso lógico, [SW.SC] Se aplican perfiles de seguridad:* Actualmente el software no cuenta con un sistema de perfiles de usuario configurado, por lo que cualquiera que pueda acceder al ERP puede acceder a toda la información crucial de la empresa. Por ello, se debe de establecer un sistema de perfiles de acuerdo con los requisitos de acceso a la información establecidos por la dirección.

- *[SW] Protección de las Aplicaciones Informáticas:* actualmente algunos departamentos cuentan con cuentas conjuntas, por lo que recomienda buscar una forma de que cada empleado cuente con su cuenta de usuario y evitar los riesgos que la compartición de cuentas pueda acarrear

(Suplantación de la identidad del usuario, Abuso de privilegios de acceso, Modificación deliberada de la información, Divulgación de información).

- *[SW.A] Copias de seguridad (backup):* actualmente ya se realizan dos copias de seguridad diarias, pero apenas se suelen revisar, por lo en las políticas se deberá establecer un periodo de revisión de validez de las copias de seguridad.

- *[SW.CM] Cambios (actualizaciones y mantenimiento):* es necesario establecer una política de actualizaciones para mejorar la estabilidad, evitar accesos no autorizados, evitar errores de software y solucionar aquellas vulnerabilidades que se vayan produciendo y solventando por parte del fabricante del software. Así como establecer una metodología de cambios de los desarrollos internos de la organización (fecha y hora del cambio, descripción de los cambios, responsable, desarrollador).

- *[H.tools.LA] Herramienta análisis logs:* el software permite establecer un sistema de logs, por lo que es imperativo configurar primero el registro de las acciones de los usuarios dentro del ERP en logs. Tras ello, una herramienta de análisis de logs, permitirá mantener un mejor control de las acciones de los usuarios y evitar fugas de información, borrados, manipulación de los datos y el no repudio de las acciones.

- *Manuales y procedimiento:* es importante desarrollar manuales con las tareas a seguir por cada departamento dentro de la aplicación ante la indisponibilidad del personal, así como los procedimientos que se emplean para la gestión de usuarios, pedidos de compra y venta, fabricaciones, cálculos de costes…

- *[PS.AT] Formación y concienciación:* es necesario formar a los empleados en el buen uso del software para que se familiaricen con el entorno y puedan adaptarse rápidamente a trabajar con ello. De esta forma, se evitaran la gran mayoría de errores involuntarios provocados por los empleados.

- *Política de Seguridad: en la política de seguridad deberán quedar reflejadas las normas de uso acerca del ERP, las responsabilidades de los empleados y los riesgos a tener en cuenta.*

- **SW006 – Suite de diseño gráfico**

Para la suite de diseño gráfico que emplea los diseñadores de la empresa para realizar los diseños, la **amenaza** que provoca el mayor riesgo es: *[A.7] Uso no previsto.*

El riesgo en si tiene que ver con la posibilidad que los empleados acaben usando el software para sus propios diseños, empleando los recursos de la empresa para su propio beneficio.

Por ello, se considera la idea de emplear la *Política de Seguridad del grupo empresarial* como **salvaguarda**, definiendo los usuarios que tienen permiso para emplear el software, las normas sobre el uso del software y los riesgos que conlleva el mal uso de este software.

- **SW007 – Antivirus**

Para el software antivirus instalado en los sistemas del grupo empresarial, las **amenazas** que provocan los mayores riesgos son: *[E.20] Vulnerabilidades de los programas (software), [E.21] Errores de mantenimiento / actualización de programas, [A.6] Abuso de privilegios de acceso, [A.11] Acceso no autorizado, [A.15] Modificación deliberada de la información.*

La mayor parte de los riesgos tiene relación con los riesgos que conlleva no tener el software de antivirus actualizado día a día, el acceso y modificación de las configuraciones de este software.

Las **salvaguardas** consideradas para mitigar el riesgo que estas amenazas provocan son: *[H.AC] Control del acceso lógico, [H.AU] Registro y auditoría, [SW] Protección de las Aplicaciones Informáticas, [SW.SC] Se aplican perfiles de seguridad, [SW.A] Copias de seguridad (backup), [SW.CM] Cambios (actualizaciones y mantenimiento), [BC] Continuidad del negocio, Política de Seguridad.*

- *[H.AC] Control del acceso lógico, [SW.SC] Se aplican perfiles de seguridad:* aplicando restricciones de acceso a la configuración se evitará la manipulación de esta, incluyendo la desactivación o eliminación del software.

- *[H.AU] Registro y auditoría:* resultaría útil mantener logs de los análisis periódicos realizados sobre las maquinas del sistema, para detectar la entrada en el sistema de archivos maliciosos o potencialmente peligrosos*.*

- *[SW] Protección de las Aplicaciones Informáticas:* se recomienda el control por directivas para que el software antivirus cliente no se pueda manipular.

- *[SW.CM] Cambios (actualizaciones y mantenimiento):* es imperativo contar con el software antivirus, evitando así, errores de mantenimiento y vulnerabilidades del software.

- *Política de Seguridad: en la política de seguridad deberán quedar reflejadas las características de los antivirus que la empresa emplea, así como los periodos donde se ejecutaran los análisis de los sistemas.*

- **SW008 – Sistema operativo**

Para los sistemas operativos de los que dispone el grupo empresarial, las **amenazas** que provocan los mayores riesgos son: *[I.5] Avería de origen físico o lógico, [E.8] Difusión de software dañino, [E.20] Vulnerabilidades de los programas (software), [A.5] Suplantación de la identidad del usuario, [A.7] Uso no previsto, [A.11] Acceso no autorizado, [A.18] Destrucción de la información.*

La mayor parte de los riesgos tiene relación con las vulnerabilidades que presentan los sistemas operativos más antiguos que ya carecen de soporte oficial y actualizaciones, pero siguen siendo necesario contar con ellas para que ciertas máquinas industriales puedan seguir funcionando. Por lo tanto, será necesario reforzar el acceso de estos sistemas todo lo posible.

Las **salvaguardas** consideradas para mitigar el riesgo que estas amenazas provocan son: *[H.AC] Control del acceso lógico, [H.AU] Registro y auditoría, [H.IA] Identificación y autenticación, [SW] Protección de las Aplicaciones Informáticas, [SW.SC] Se aplican perfiles de seguridad, [SW.A] Copias de seguridad (backup), [SW.CM] Cambios (actualizaciones y mantenimiento), [H.tools.AV] Herramienta contra código dañino, [BC] Continuidad del negocio, Política de Seguridad.*

- *[H.AC] Control del acceso lógico, [SW.SC] Se aplican perfiles de seguridad, [H.IA] Identificación y autenticación:* actualmente solo se permite a los usuarios administradores realizar cambios en el software y en las configuraciones de los sistemas operativos. La gran mayoría de cambios se realizan mediante las directivas de grupo.

- *[H.AU] Registro y auditoría:* es de gran importancia conservar un registro de los accesos en los sistemas operativos, para mitigar la amenaza de accesos no autorizados.

- *[SW] Protección de las Aplicaciones Informáticas:* los sistemas operativos más antiguos deben de reforzarse con el fin de que no se puedan explotar sus vulnerabilidades para acciones que puedan resultar perjudiciales para la organización.

- *[SW.A] Copias de seguridad (backup):* el plan de copias de seguridad deberá de contemplar realizar copias de la configuración de los sistemas operativos de las máquinas servidoras, para que en el caso de un desastre, se pueda reestablecer cuanto antes recuperando así todas las funciones, servicios y elementos de configuración que se incluyen en este sistema.

- *[SW.CM] Cambios (actualizaciones y mantenimiento):* la política de seguridad debería de contemplar que los sistemas operativos se actualicen de forma regular para siempre contar con las últimas actualizaciones de seguridad.

- *[H.tools.AV] Herramienta contra código dañino:* una herramienta así permitirá reforzar los sistemas operativos ante la aparición de código malicioso.

- *[BC] Continuidad del negocio:* en los planes de continuidad de negocio se deben de establecer planes de recuperación de los sistemas operativos de los servidores ante fallos que fuercen el reinicio de la maquina o directamente se requiera instalar un nuevo servidor para realizar un reemplazo. Estos planes deben de considerar la recuperación de los sistemas operativos, las funcionalidades y servicios al estado de operación óptimo para la buena operación de la infraestructura informática empresarial.

- *Política de Seguridad:* en la política de seguridad deberán quedar reflejadas las normas de uso acerca de los diferentes sistemas operativos de la organización, así como las características y riesgos a tener en cuenta.

- **SW009 – Sistema de backup**

Para el software de backup, **los riesgos encontrados son demasiado bajos**, por lo que en este caso la organización ha decidido que su protección no tiene prioridad y los riesgos serán **aceptados**.

- **SW011 – Software de fabricación, SW012 – Software gestión de proyectos**

Estos archivos se refieren a las aplicaciones software propietarias de la empresa que se emplean para la gestión de proyectos del grupo empresarial y el sistema de ejecución de la fabricación (MES). Al tratarse de información crítica para la empresa, la seguridad es imperativa.

En estos activos, las **amenazas** que provocan los mayores riesgos son: *[E.1] Errores de los usuarios, [E.2] Errores del administrador, [E.18] Destrucción de la información, [E.20] Vulnerabilidades de los programas (software), [E.21] Errores de mantenimiento / actualización de programas, [A.6] Abuso de privilegios de acceso, [A.8] Difusión de software dañino, [A.15] Modificación deliberada de la información, [A.18] Destrucción de la información, [A.19] Divulgación de información.*

La gran mayoría de estas amenazas corresponden a posibles accesos no autorizados, errores en las configuraciones de los programas y vulnerabilidades de las aplicaciones.

Por lo tanto, las **salvaguardas** que se contemplan son: *[H.AC] Control del acceso lógico, [H.AU] Registro y auditoría, [SW] Protección de las Aplicaciones Informáticas, [SW.SC] Se aplican perfiles de seguridad, [SW.A] Copias de seguridad (backup), [SW.CM] Cambios (actualizaciones y mantenimiento), [H.tools.LA] Herramienta análisis logs, [BC] Continuidad del negocio, Política de Seguridad.*

- *[H.AC] Control del acceso lógico, [SW.SC] Se aplican perfiles de seguridad:* actualmente estas aplicaciones cuentan con un sistema de permisos de usuario realizado de forma informal, por lo que se recomendaría realizar un estudio de los grupos de usuarios que trabajan con el software, para implementar un sistema de perfiles de seguridad informal. De forma ideal, se recomendaría que estos perfiles de usuario se tomasen de los perfiles de usuario desarrollados en el ERP, para evitar la duplicidad de configuraciones.

- *[H.AU] Registro y auditoría:* es de gran importancia conservar un registro de los accesos y acciones de los usuarios, para evitar abusos de privilegios y el no repudio.

- *[SW] Protección de las Aplicaciones Informáticas:* establecer una protección en estas aplicaciones podrá ayudar a reforzar la seguridad de estas ante posibles vulnerabilidades, difusión de software dañino o errores que puedan cometer los usuarios.

- *[SW.A] Copias de seguridad (backup):* actualmente ya se realizan copias de seguridad de la información con la que trabajan estas aplicaciones, por lo que sería interesante detallar en plan de copias de seguridad los requisitos de copias que este software requiere.

- *[SW.CM] Cambios (actualizaciones y mantenimiento):* actualmente los cambios en estos activos software se realiza de forma informal, sin documentación ninguna. Se recomienda establecer planes de actualización, para formalizar la realización de actualizaciones en agrupaciones preparadas y realizar el aviso a todos los responsables. La documentación de los cambios debe de incluir: las funcionalidades añadidas, modificadas o eliminadas, junto al responsable, el desarrollador y las comprobaciones realizadas.

- *[H.tools.LA] Herramienta análisis logs:* actualmente el software cuenta con un sistema de logs muy rudimentario, por lo que una herramienta de análisis de logs ayudaría a darle valor a los logs que generan estas aplicaciones, permitiendo la detección temprana de errores.

- *[BC] Continuidad del negocio*: en los planes de continuidad de negocio se deben de establecer planes de recuperación en el caso de pérdida de información.

- *Política de Seguridad:* en la política de seguridad deberán quedar reflejadas las normas de uso acerca de este software, las responsabilidades de los empleados y los riesgos a tener en cuenta.

8.1.4. [HW] Hardware (tratamiento del riesgo)

- **HW003 - Ordenadores diseño**

Para los ordenadores dedicados al diseño industrial de los que dispone el grupo empresarial, las **amenazas** que provocan los mayores riesgos son: *[I.1] Fuego, [I.2] Daños por agua, [I.5] Avería de origen físico o lógico, [A.25] Robo.*

La mayor parte de los riesgos tiene relación con riesgos industriales y la posibilidad de robo de estos equipos, ya que estas máquinas presentan un coste muy elevado.

Las **salvaguardas** consideradas para mitigar el riesgo que estas amenazas provocan son: *[D.A] Copias de seguridad de los datos, [HW] Protección Equipos Informáticos, [HW.A] Aseguramiento de la disponibilidad, Política de Seguridad*.

- *[D.A] Copias de seguridad de los datos:* actualmente se realizan copias de seguridad de los datos, por lo que esta salvaguarda ayuda a mitigar los riesgos que afecten a la disponibilidad.

- *[HW] Protección Equipos Informáticos:* es necesario contar con un plan para proteger los equipos informáticos, por lo que se recomienda compartir los riesgos que afecten a la disponibilidad mediante la contratación de un seguro para estos equipos.

- *[HW.A] Aseguramiento de la disponibilidad:* contar con algún equipo de reserva (no necesariamente con las mismas especificaciones) puede ayudar a asegurar la disponibilidad, esta salvaguarda permitirá suplir los riesgos que afecten a la disponibilidad de estos equipos.

- *Política de Seguridad:* en la política de seguridad deberán quedar reflejadas las normas de uso del hardware, las responsabilidades de uso y los riesgos a tener en cuenta.

- **HW006 - NAS, HW018 - Servidor de copias**

Estos archivos se refieren al servidor donde se realizan y almacenan parte de las copias que se realizan y el servidor de almacenamiento en red (NAS) donde se almacenan la mayoría de la documentación propietaria de la empresa. Al contener información crítica para la empresa, la seguridad es imperativa.

En estos activos, las **amenazas** que provocan los mayores riesgos son: *[N] Desastres naturales, [I.1] Fuego, [I.2] Daños por agua, [I.*] Desastres naturales, [I.3] Contaminación mecánica, [I.5] Avería de origen físico o lógico, [I.6] Corte de suministro eléctrico, [I.7] Condiciones inadecuadas de temperatura o humedad, [E.23] Errores de mantenimiento / actualización de equipos, [E.24] Caída del sistema por agotamiento de recursos, [E.25] Perdida de equipos, [A.6] Abuso de privilegios de acceso, [A.7] Uso no previsto, [A.11] Acceso no autorizado, [A.24] Denegación de servicio, [A.25] Robo, [A.26] Ataque destructivo*

La gran mayoría de estas amenazas corresponden a posibles accesos no autorizados, amenazas industriales y no contar con una ubicación segura a prueba de intrusiones.

Por lo tanto, las **salvaguardas** que se contemplan son:

- *[H.AC] Control acceso lógico*: actualmente para acceder a los servidores ya se requiere del uso de una contraseña o ser miembro del grupo de administradores para acceder, pero para asegurar completamente el acceso lógico sería recomendable usar certificados autogenerados, con ello podrían evitarse las amenazas de accesos lógicos no deseados.

- *[L.AC] Control acceso físico*: sería necesario realizar un control del acceso físico para evitar riesgos que involucren contacto físico directo con las maquinas, ya que actualmente no se cuenta con ninguna medida para proteger estos activos. El acceso solo debe ser permitido al personal autorizado y responsable del grupo empresarial.

- *[D.C] Cifrado de la información*: la información contenida en el servidor de copias y en el NAS es de vital importancia, por lo que se recomendaría realizar un cifrado de la información contenida en los soportes o por lo menos, de aquella de una importancia más sensible y critica para el grupo empresarial.

- *[HW.A] Aseguramiento de la disponibilidad*: para asegurar la disponibilidad se podría disponer de servidores secundarios que pudiesen realizar la labor de servidor de copias o NAS en el caso de que los principales sufriesen la materialización de alguna amenaza que los dejase inoperativos. También podría considerarse la configuración de las copias de seguridad contra un servicio en *Cloud o una combinación de Cloud y maquina secundaria.*

- *[BC] Continuidad del negocio*: en los planes de continuidad de negocio se deben de establecer planes de recuperación en el caso de pérdida de información.

- *Política de Seguridad*: en la política de seguridad deberán quedar reflejadas las características del servidor de copias y del NAS, así como los periodos donde se ejecutaran los las copias, los usuarios que cuentan con acceso.

- *CPD Dedicado*: al contar con un CPD dedicado se podrían reducir los riesgos relacionados con las amenazas industriales, los accesos físicos no autorizados y las condiciones inadecuadas de temperatura y humedad.

- **HW009 - Servidores físicos, HW010 - Servidores virtualizados**

Estos archivos se refieren a las aplicaciones software propietarias de la empresa que se emplean para la gestión de proyectos del grupo empresarial y el sistema de ejecución de la fabricación (MES). Al tratarse de información crítica para la empresa, la seguridad es imperativa.

En estos activos, las **amenazas** que provocan los mayores riesgos son: *[N] Desastres naturales, [I.1] Fuego, [I.2] Daños por agua, [I.*] Desastres naturales, [I.3] Contaminación mecánica, [I.5] Avería de origen físico o lógico, [I.6] Corte de suministro eléctrico, [I.7] Condiciones inadecuadas de temperatura o humedad, [E.2] Errores del administrador, [E.23] Errores de mantenimiento / actualización de equipos, [E.24] Caída del sistema por agotamiento de recursos, [E.25] Perdida de equipos, [A.6] Abuso de privilegios de acceso, [A.7] Uso no previsto, [A.11] Acceso no autorizado, [A.24] Denegación de servicio, [A.25] Robo, [A.26] Ataque destructivo.*

La gran mayoría de estas amenazas corresponden a posibles accesos no autorizados, errores en las configuraciones de los programas y vulnerabilidades de las aplicaciones.

Por lo tanto, las **salvaguardas** que se contemplan son: *[D.A] Copias de seguridad de los datos, [H.AC] Control acceso lógico, [L.AC] Control acceso físico, [H.AU] Registro, auditoría, [HW] Protección Equipos Informáticos, [D.C] Cifrado información, [H.tools.LA] Herramienta análisis logs, [H.tools.AV] Herramienta contra código dañino, [HW.A] Aseguramiento de la disponibilidad, [HW.CM] Cambios (actualizaciones y mantenimiento), [BC] Continuidad del negocio, Política de Seguridad, CPD Dedicado*.

- *[D.A] Copias de seguridad de los datos:* la información almacenada en estos dispositivos es crucial para el desempeño de las labores de la empresa, por lo que se debe realizar copias de seguridad diarias en una o más ocasiones, para asegurar la disponibilidad.

- *[H.AC] Control acceso lógico:* actualmente para acceder a los servidores ya se requiere del uso de una contraseña o ser miembro del grupo de administradores para acceder, pero para

asegurar completamente el acceso lógico sería recomendable usar certificados autogenerados, con ello podrían evitarse las amenazas de accesos lógicos no deseados.

- *[L.AC] Control acceso físico:* sería necesario realizar un control del acceso físico para evitar riesgos que involucren contacto físico directo con las maquinas, ya que actualmente no se cuenta con ninguna medida para proteger estos activos. El acceso solo debe ser permitido al personal autorizado y responsable del grupo empresarial.

- *[H.AU] Registro, auditoría:* es de gran importancia conservar un registro de los accesos (tanto los correctos como los intentos fallidos) y acciones de los usuarios, para evitar accesos no autorizados, el abuso de privilegios y el no repudio.

- *[HW] Protección Equipos Informáticos:* para proteger los servidores de posibles amenazas físicas se recomienda el uso de un armario rack, para evitar posibles incidentes y permitir al administrador una mejor gestión de los dispositivos.

- *[D.C] Cifrado información:* se requiere de salvaguardas de este tipo para proteger la confidencialidad de la información que guardan los servidores ante amenazas de fugas de información, robo o divulgaciones de información. Se debe de organizar y cifrar la información más sensible.

- *[H.tools.LA] Herramienta análisis logs, [H.tools.AV] Herramienta contra código dañino:* como medidas de seguridad preventivas se plantea la instalación de herramientas que permitan el análisis de los logs del sistema y contra las aplicaciones que puedan contener código malicioso.

- *[HW.A] Aseguramiento disponibilidad:* en los servidores se ejecutan funciones críticas para el buen hacer del grupo empresarial, por lo que es imperativo contar con un mecanismo de alta disponibilidad como contingencia ante incidentes graves. Se propone la instalación de un servidor que actúe como clúster o secundario de los demás servidores (o del principal) y en caso de necesidad pueda desempeñar de forma temporal las misma funcionalidades que el original.

- *[HW.CM] Cambios (actualizaciones y mantenimiento):* se incluye una política de cambios que permita mantener actualizados los servidores con las últimas actualizaciones de seguridad tanto en hardware como en software. Se realizará un registro de todas las actualizaciones con las modificaciones y los responsables.

- *[BC] Continuidad del negocio:* en los planes de continuidad de negocio se deben de establecer los planes de contingencia y recuperación de los servidores, explicando paso a paso los pasos a seguir para volver a dejar el sistema en un estado óptimo.

- *Política de Seguridad:* en la política de seguridad deberán quedar reflejadas las características de los servidores (tanto los físicos como los virtualizados) con las finalidades a las que sirven y los responsables de su correcto funcionamiento.

- *CPD Dedicado:* al contar con un CPD dedicado se podrían reducir los riesgos relacionados con las amenazas industriales, los accesos físicos no autorizados y las condiciones inadecuadas de temperatura y humedad.

- **HW007 - Router, HW011 - Switch, HW014 - Mini-switch**

Estos archivos se refieren a las aplicaciones software propietarias de la empresa que se emplean para la gestión de proyectos del grupo empresarial y el sistema de ejecución de la fabricación (MES). Al tratarse de información crítica para la empresa, la seguridad es imperativa.

En estos activos, las **amenazas** que provocan los mayores riesgos son: *[N] Desastres naturales, [I.1] Fuego, [I.2] Daños por agua, [I.*] Desastres naturales, [I.3] Contaminación mecánica, [I.4] Contaminación electromagnética, [I.5] Avería de origen físico o lógico, [I.6] Corte de suministro eléctrico, [I.7] Condiciones inadecuadas de temperatura o humedad, [E.2] Errores del administrador, [E.23] Errores de mantenimiento / actualización de equipos, [E.24] Caída del sistema por agotamiento de recursos, [E.25] Perdida de equipos, [A.6] Abuso de privilegios de acceso, [A.7] Uso no previsto, [A.11] Acceso no autorizado, [A.23] Manipulación de los equipos, [A.24] Denegación de servicio, [A.25] Robo, [A.26] Ataque destructivo*

La gran mayoría de estas amenazas corresponden a posibles accesos no autorizados, errores en las configuraciones de los programas y vulnerabilidades de las aplicaciones.

Por lo tanto, las **salvaguardas** que se contemplan son: *[SW.A] Copia de seguridad de la configuración, [H.AC] Control acceso lógico, [L.AC] Control acceso físico, [H.IA] Identificación y autenticación, [HW] Protección Equipos Informáticos, [HW.A] Aseguramiento disponibilidad, [HW.CM] Cambios (actualizaciones y mantenimiento), [BC] Continuidad del negocio, Política de Seguridad, CPD Dedicado*.

- *[SW.A] Copia de seguridad de la configuración*: en ambos casos es necesario tener guardada una copia de la configuración como contingencia siendo parte de la política de seguridad. Es considerada como información sensible, por lo que deberá ser también protegida adecuadamente.

- *[H.AC] Control acceso lógico, [H.IA] Identificación y autenticación:* actualmente para acceder a los dispositivos de red ya se requiere del uso de una contraseña o ser miembro del grupo de

administradores para acceder, pero para asegurar completamente el acceso lógico sería recomendable usar certificados autogenerados, con ello podrían evitarse las amenazas de accesos lógicos no deseados.

- *[L.AC] Control acceso físico:* sería necesario realizar un control del acceso físico para evitar riesgos que involucren contacto físico directo con las maquinas, ya que actualmente no se cuenta con ninguna medida para proteger estos activos. El acceso solo debe ser permitido al personal autorizado y responsable del grupo empresarial.

- *[HW] Protección Equipos Informáticos:* para proteger los dispositivos de red se recomienda el uso de un armario rack, para evitar posibles incidentes y permitir al administrador una mejor gestión de los dispositivos.

- *[HW.A] Aseguramiento disponibilidad:* para asegurar la disponibilidad sería necesario contar con un router o switches secundarios bien configurados que pudiesen desempeñar la misma labor mientras los principales se encuentran inactivos.

- *[HW.CM] Cambios (actualizaciones y mantenimiento):* es necesario mantener un registro en los cambios de la configuración de los dispositivos para mitigar riesgos ante las amenazas de posibles errores que pudiesen ser cometidos por el administrador o problemas en los mantenimientos o configuraciones. Establecer además un plan de mantenimiento periódico para comprobar el correcto estado de funcionamiento de los dispositivos.

- *[BC] Continuidad del negocio:* en los planes de continuidad de negocio se deben de establecer planes de recuperación en el caso de un incidente que afecte al router o a alguno de los switch. En el caso del router, se tendrá que pedir al proveedor un dispositivo nuevo al que se le pueda cargar las configuraciones del router. En el caso del switch, simplemente se requerirá la instalación de uno de los switch de reserva. La política debe garantizar las instrucciones para llevar a cabo el cambio.

- *Política de Seguridad:* en la política de seguridad deberán quedar reflejadas las políticas a implementar respecto a estos dispositivos, como sus configuraciones, los responsables, ubicación, medidas de seguridad y los periodos de mantenimiento.

- *CPD Dedicado:* al contar con un CPD dedicado se podrían reducir los riesgos relacionados con las amenazas industriales, los accesos físicos no autorizados y las condiciones inadecuadas de temperatura y humedad.

- **HW016 – Terminales**

Para las terminales, que son aquellos ordenadores conectados directamente a las máquinas con el software que requieren las máquinas para su buen funcionamiento, las **amenazas** que provocan los mayores riesgos son: *[I.1] Fuego, [I.2] Daños por agua, [I.3] Contaminación mecánica*.

La mayor parte de los riesgos que sufren estas máquinas son de carácter industrial, ya que se encuentran en contacto directo con la actividad industrial pudiendo verse afectadas de forma negativa por los riesgos que las amenazas industriales conllevan.

Las **salvaguardas** consideradas para mitigar el riesgo que estas amenazas provocan son: *[D.A] Copias de seguridad de los datos, [HW] Protección Equipos Informáticos, [BC] Continuidad del negocio, Política de Seguridad*.

- *[D.A] Copias de seguridad de los datos*: el plan de copias de seguridad deberá de contemplar contar con copias de la configuración de los sistemas operativos de las máquinas terminales, para que en el caso de un desastre, se pueda reestablecer cuanto antes recuperando así todas las funciones, servicios y elementos de configuración que se incluyen en este sistema.

- *[HW] Protección Equipos Informáticos:* algunas de las terminales de las máquinas son responsabilidad de empresas externas, por lo que el riesgo es compartido. Aun así, se cuenta con instalaciones de extintores y medidas anti-incendios.

- *[BC] Continuidad del negocio:* en los planes de continuidad de negocio se deben de establecer planes de recuperación en el caso de que una terminal resulte dañada y los pasos que se deben de seguir para recuperar la terminal y reestablecer el servicio de la máquina industrial.

- *Política de Seguridad:* en la política de seguridad deberán quedar reflejadas las normas de uso de las terminales, las responsabilidades de los empleados y los riesgos a tener en cuenta.

8.1.5. [COM] Redes de comunicaciones (tratamiento del riesgo)

- **COM001 – Red local LAN**

Para la red de área local del grupo empresarial, las **amenazas** que provocan los mayores riesgos (afectando especialmente a las dimensiones de disponibilidad y confidencialidad) son: *[I.8] Fallo de servicios de comunicaciones, [E.2] Errores del administrador, [E.9] Errores de re-*

encaminamiento, [E.24] Caída del sistema por agotamiento de recursos, [A.5] Suplantación de la identidad del usuario, [A.6] Abuso de privilegios de acceso, [A.7] Uso no previsto, [A.9] Re-encaminamiento de mensajes, [A.10] Alteración de secuencia, [A.11] Acceso no autorizado, [A.12] Análisis de tráfico, [A.14] Interceptación de información (escucha), [A.15] Modificación deliberada de la información, [A.19] Divulgación de información, [A.24] Denegación de servicio.

La mayor parte de los riesgos tiene relación con la posibilidad de accesos no autorizados de intrusos o posibles caídas de la red por falta de recursos por abuso de las capacidades de la red. Por lo tanto, las medidas que se puede adoptar pretenden reforzar la seguridad de la red (arquitectura y acceso), uso de las redes, acciones sospechosas, prevención y alerta

Las **salvaguardas** consideradas para mitigar el riesgo que estas amenazas provocan son:

- *[H.AC] Control de acceso lógico, [L.AC] Control de los accesos físicos, [COM.SC] Se aplican perfiles de seguridad*: el acceso a la red empleando mecanismos de control de la seguridad de acceso, la protección de las conexiones físicas a la red y el uso de perfiles de usuario junto con el uso de certificados, ayudan a reducir los riesgos de abuso de privilegios, accesos no autorizados, suplantación de identidades y las posibles consecuencias que puede acarrear como ataques de denegación de servicio (DoS) o el uso de la red para acciones maliciosas.

- *[H.AU] Registro y auditoría:* el registro de conexiones permitirá analizar los posibles incidentes, para determinar el impacto de un ataque, garantizar el no repudio y comprobar conexiones sospechosas en la red o el uso no previsto de esta.

- *[COM.DS] Segregación de la red en dominios:* la división de una red en diferentes dominios puede ayudar a separar las diferentes redes del grupo empresarial que actualmente se encuentran agrupadas bajo la misma red, suponiendo un gran riesgo permitiendo la propagación de software malicioso, la escucha y el análisis de todo el tráfico corporativo.

- *[COM.AUT] Autenticación del canal*: asegurar la autenticidad del canal entre los dispositivos más cruciales, permitirá evitar suplantaciones de identidad en la red.

- *[COM.I] Protección de la integridad de los datos intercambiados*: esta salvaguarda permitirá reforzar la integridad de los datos que transcurren a través de la red, para evitar manipulaciones de la información y alteraciones de secuencia.

- *[COM.A] Aseguramiento de la disponibilidad*: en el caso de problemas de la red, disponer de otra red en la que se encuentren conectadas los componentes más importantes de la organización.

- *[COM.C] Protección criptográfica:* el uso de protocolos seguros (como SSL o HTTPS) para proteger el tráfico de la red, permitirá reforzar la red e impedir que se realicen escuchas o análisis del tráfico.

- *[COM.CM] Cambios (actualizaciones y mantenimiento):* Las actualizaciones y mantenimiento de los diferentes elementos de la red son cruciales para asegurar que se mitigan las vulnerabilidades que se hayan corregido por parte de los fabricantes. Además, del cambio de aquellos componentes obsoletos y amortizados, que pasan a conllevar un riesgo demasiado elevado para la seguridad de la red.

- *[H.tools.IDS] IDS/IPS: Herramienta de detección / prevención de intrusión*: Una salvaguarda de este tipo ayudará a la detección y prevención de amenazas. Esta herramienta se puede integrar con el firewall, lo que permite detectar y bloquear intrusiones, ataques y comportamientos sospechosos.

- *[H.tools.CC] Herramienta de chequeo de configuración*: esta salvaguarda permitirá comprobar manipulaciones de la configuración y avisar de los posibles cambios que se realicen, lo que permite detectar manipulaciones indebidas.

- *Política de seguridad*: La política de seguridad permitirá reducir el riesgo que puede producir un mal uso de la red, como la descarga de contenido ilegal, de fuentes dudosas o archivos muy pesados, acceso a dominios no recomendados, el uso abusivo de los recursos de la red, el envío de archivos adjuntos con información sensible hacia el exterior de la empresa.

- **COM005 – Fibra**

Los mayores riesgos de seguridad que amenazan a la fibra que provee al grupo empresarial de conexión a Internet, se encuentran relacionados con las siguientes **amenazas**: *[I.8] Fallo de servicios de comunicaciones, [E.9] Errores de re-encaminamiento, [E.24] Caída del sistema por agotamiento de recursos, [A.5] Suplantación de la identidad del usuario, [A.6] Abuso de privilegios de acceso, [A.7] Uso no previsto, [A.9] Re-encaminamiento de mensajes, [A.11] Acceso no autorizado, [A.12] Análisis de tráfico, [A.14] Interceptación de información (escucha), [A.19] Divulgación de información, [A.24] Denegación de servicio*.

Gran parte de estos riesgos se deben a la posibilidad de fallos en el servicio de comunicaciones.

Las **salvaguardas** consideradas para reducir el riesgo que estas amenazas provocan son: *[L.AC] Control de los accesos físicos, [COM.A] Aseguramiento de la disponibilidad, Plan de contingencia, Política de Seguridad.*

- *[L.AC] Control de los accesos físicos*: este control impedirá que personal no autorizado pueda acceder a los dispositivos que proveen acceso a la fibra.

- *[COM.A] Aseguramiento de la disponibilidad*: esta salvaguarda dispondrá de un acceso a Internet alternativo que poder usar en el caso de que la comunicación por fibra haya caído.

- *Plan de contingencia*: permitirán determinar qué acciones llevar a cabo y por quien en caso de problemas con la conexión a Internet.

- *Política de seguridad*: permitirán establecer unas normas de uso correctas. Al igual que en la red LAN, estas normas permitirán reducir en gran parte los riesgos.

Los riesgos en los que la organización no tiene la responsabilidad de aplicar salvaguardas (*[E.9] Errores de re-encaminamiento, [A.9] Re-encaminamiento de mensajes, [A.12] Análisis de tráfico, [A.14] Interceptación de información (escucha), [A.24] Denegación de servicio):* estos riesgos quedan compartidos por la empresa proveedora del servicio de Internet.

8.1.6. [MEDIA] Soportes de información (tratamiento del riesgo)

- **MEDIA001 – Discos duros extraíbles**

Para los discos duros empleados por el grupo empresarial para realizar las copias de seguridad semanales, las **amenazas** que provocan los mayores riesgos son: *[I.1] Fuego, [I.2] Daños por agua, [E.2] Errores del administrador, [E.15] Alteración accidental de la información, [E.18] Destrucción de la información, [E.19] Fugas de información, [E.25] Perdida de equipos, [A.7] Uso no previsto, [A.11] Acceso no autorizado, [A.15] Modificación deliberada de la información, [A.25] Robo*.

Gran parte de estos riesgos se deben a posibilidad del acceso no autorizado a la información de los discos, ya que se almacenan en un lugar a la vista de cualquiera sin ninguna clase de vigilancia ni cierres de seguridad. Además, se dispone de una cantidad muy limitada de estos discos.

Las **salvaguardas** consideradas para reducir el riesgo que estas amenazas provocan son: [MP] Protección de los Soportes de Información, [MP.end] Destrucción de soportes, [MP.A] Aseguramiento de la disponibilidad, [MP.IC] Protección criptográfica del contenido, Política de Seguridad.

Estas salvaguardas buscan proteger los discos buscando una localización segura donde poder almacenarlos lejos de posibles peligros de origen industrial y accesos no autorizados, proteger

el contenidos de los discos para que no puedan ser accesibles por cualquiera que acceda a ellos, asegurar que exista una reserva de discos de almacenamiento y asegurar que cuando los discos sean dados de baja, se proceda a su destrucción para evitar que se pueda recuperar cualquier dato de estos.

Dentro de la política de seguridad de la empresa deben existir directrices del uso y preservación de los discos de almacenamiento de las copias de seguridad. Por ejemplo, establecer siempre un uso en concreto, que se encuentren cifrados, los intervalos entre copias, la comprobación que debe realizar el responsable, los lugares donde almacenarlos…

- **MEDIA002 – Blue-Ray**

Para los discos blue-ray empleados por el grupo empresarial para realizar las copias de seguridad anuales, las **amenazas** que provocan los mayores riesgos son: *[E.2] Errores del administrador, [E.19] Fugas de información, [E.25] Perdida de equipos, [A.11] Acceso no autorizado, [A.25] Robo*.

Gran parte de estos riesgos se deben a posibilidad del acceso no autorizado a la información de los discos, ya que se almacenan en un lugar a la vista de cualquiera sin ninguna clase de vigilancia ni cierres de seguridad.

Las **salvaguardas** consideradas para reducir el riesgo que estas amenazas provocan son: [MP] Protección de los Soportes de Información, [MP.end] Destrucción de soportes, [MP.A] Aseguramiento de la disponibilidad, [MP.IC] Protección criptográfica del contenido, Política de Seguridad.

Estas salvaguardas buscan proteger los discos buscando una localización segura donde poder almacenarlos lejos de posibles accesos no autorizados, proteger el contenidos de los discos para que no puedan ser accesibles por cualquiera que acceda a ellos y asegurar que cuando los discos sean dados de baja, se proceda a su destrucción para evitar que se pueda recuperar cualquier dato de estos.

Dentro de la política de seguridad de la empresa deben existir directrices del uso y preservación de los discos de almacenamiento de las copias de seguridad anuales. Por ejemplo, quien debe tener acceso a ellos, cuantos años deben conservarse los discos antes de proceder a su destrucción, que se encuentren cifrados, los lugares donde almacenarlos…

8.1.7. [L] Instalaciones (tratamiento del riesgo)

- **L001 - Nave principal**

Para la nave principal del grupo empresarial las **amenazas** que provocan los mayores riesgos son: *[N] Desastres naturales, [I.1] Fuego, [E.15] Alteración accidental, [E.18] Destrucción de la información, [E.19] Fugas de información, [A.11] Acceso no autorizado, [A.15] Modificación deliberada, [A.18] Destrucción de la información, [A.19] Divulgación de información, [A.26] Ataque destructivo, [A.27] Ocupación enemiga*.

En la Nave principal del grupo empresarial es donde se encuentran los activos de mayor valor, por lo tanto, lo que le suceda a este edificio puede repercutir en daños graves para todo el grupo empresarial. La mayor parte de estos riesgos tienen que ver con el control de acceso físico. El edificio no cuenta con un registro de registro de acceso, motivo, persona visitada, horario. Tampoco cuenta con personal para recibir a las visitas y la puerta de acceso suele encontrarse abierta la mayor parte del tiempo. Hay veces que las visitas entran en el edificio y se dirigen directamente a los despachos de forma independiente. Existen algunos riesgos referentes a la posibilidad de incendio, ya que la empresa trabaja con una gran cantidad de máquinas y materiales de fácil combustión. Aunque la empresa ya cuenta con instalación de extintores por todas las zonas de peligro, por lo que aplicar la salvaguarda no será necesario.

Las **salvaguardas** consideradas para reducir el riesgo que estas amenazas provocan son: *[L] Protección de las Instalaciones, [L.AC] Control de los accesos físicos, Política de Seguridad de la empresa, Registro incidentes de seguridad.*

Estas salvaguardas tienen el objetivo de reforzar el control de acceso y disponer de unas políticas que ayuden a establecer una normativa sobre el acceso y circulación de personal externo por las instalaciones, además de establecer unos límites de acceso al personal, clientes y visitas. La empresa ya cuenta con un sistema de video vigilancia para cubrir las zonas de acceso a la nave, por lo que esta salvaguarda ya se encuentra dispuesta.

- **L005 – CPD**

Para la localización del actual CPD del grupo empresarial, siendo esta sala el lugar donde residen actualmente los servidores de la empresa y los elementos físicos de la red, las **amenazas** que provocan los mayores riesgos son: *[N] Desastres naturales, [I.1] Fuego, [E.18] Destrucción de la información, [E.19] Fugas de información, [A.7] Uso no previsto, [A.11] Acceso no autorizado,*

[A.18] Destrucción de la información, [A.19] Divulgación de información, [A.26] Ataque destructivo, [A.27] Ocupación enemiga.

Siendo el CPD el lugar donde residen los servidores de la empresa y los elementos físicos de la red, el nivel de riesgo es consecuencia de los elementos que alberga. Esta localización actualmente se encuentra en un gran riesgo, ya que se accede a través de una puerta sin cerradura desde la cafetería, por lo que es accesible por cualquier persona (personal, clientes, visitas). Actualmente, esta localización también se emplea para otros muchos propósitos como el de almacén y cuarto de la limpieza, por lo que la probabilidad de que se produzcan incidentes no intencionados es muy elevada.

Las **salvaguardas** consideradas para reducir el riesgo que estas amenazas provocan son: *[L] Protección de las Instalaciones, [L.AC] Control de los accesos físicos, [AUX.AC] Climatización, [AUX.wires] Protección del cableado, Política de Seguridad de la empresa, Registro incidentes de seguridad.*

Estas salvaguardas tienen el objetivo de reforzar el control de acceso al CPD, limitando solo el acceso al personal autorizado, establecer una localización no tan transitada y ofrecer una fuerte protección a los activos que se alojan en esta ubicación, ofreciendo medidas anti-incendios, control de la temperatura y humedad, protección ante problemas eléctricos.

Para todas las instalaciones, en el caso del riesgo ante desastres naturales, no se establece ninguna salvaguarda en concreto, el riesgo es asumido, por lo que se contratará un seguro acorde para compartir riesgo.

Actualmente, el grupo empresarial cuenta con el servicio de una empresa de seguridad, por lo que el riesgo ante ataque destructivo y ocupación enemiga se encuentra compartido con la empresa de seguridad.

Adicionalmente, es de gran importancia que todos los empleados sean formados en materia de seguridad, con el objetivo de concienciar acerca de las amenazas y riesgos que deben de conocer para poder hacerles frente y evitar fugas de información fortuitas. Además, es de gran importancia hacer al personal conocedor de la normativa en materia de seguridad sobre la gestión de la información que se debe de cumplir.

8.1.8. [P] Personal (tratamiento del riesgo)

Para todos los activos referidos al personal las **amenazas** que provocan los mayores riesgos son: *[E.19] Fugas de información, [E.28] Indisponibilidad del personal y [A.30] Ingeniería social (picaresca)*.

Se trata del riesgo asociado a la revelación de información a través de la intervención directa del personal y el riesgo derivado de la disponibilidad del personal.

Las **salvaguardas** consideradas para reducir el riesgo que estas amenazas provocan son: *[PS.AT] Formación y concienciación, [PS.A] Aseguramiento de la disponibilidad, Política de Seguridad, Plan de contingencia, Elaboración de procedimientos.*

Es de gran importancia que todos los empleados sean formados en materia de seguridad, con el objetivo de concienciar acerca de las amenazas y riesgos que deben de conocer para poder hacerles frente y evitar fugas de información fortuitas. Además, es de gran importancia hacer al personal conocedor de la normativa en materia de seguridad sobre la gestión de la información que se debe de cumplir.

En cuanto a la disponibilidad del personal, es necesario contar con los procesos documentados mediante procedimientos y además de contar con planes de contingencia ante diversas situaciones de indisponibilidad del personal (como en el caso de la ausencia de responsables).

Implementando estas salvaguardas, se estima que su efectividad en la reducción del impacto y riesgo de las amenazas pueda ser cercana a un 50%, dejando los riesgos en niveles aceptables por el grupo empresarial.

8.2. Planes de seguridad

A continuación, presentamos la lista de los planes o programas de seguridad ordenados según orden de prioridad recomendada que deben implementarse para mejorar la seguridad de la empresa. Estos planes formarán parte del Plan Director de la Empresa, ya que son los que más prioridad acarrean.

8.2.1. Programa CPD dedicado

Tabla 150. Programa de seguridad - CPD dedicado

CPD DEDICADO	**PRIORIDAD ALTA**
Objetivos:	• Habilitar un espacio físico destinado únicamente a la instalación de un CPD, exclusivo para servidores y elementos críticos de la red. • Restringir el acceso solo al personal autorizado responsable. • Adecuar las condiciones de temperatura, humedad y medidas anti-incendios.
Activos afectados:	L005-CPD Además del cableado red local y resto de dispositivos reubicados. HW006-NAS, HW009-Servidores, HW018-Servidor de copias, HW007-Router, HW011-Switch, AUX003-Sai, AUX004-Equipo de climatización
Participantes:	Gerencia y responsable TI
Salvaguarda:	[L.AC] Control de los accesos físicos [AUX.start] Sistema anti-incendios [AUX.AC] Climatización [AUX.wires] Protección del cableado [AUX.start] Sistema de video vigilancia [AUX.start] Sistema de control de acceso
Descripción:	Actualmente la empresa dispone de una habitación donde se encuentran los servidores de la empresa y los elementos críticos de la red. Pero esta habitación no presenta ninguna medida que impida el acceso no autorizado (cualquier persona puede abrir la puerta), no dispone del acondicionamiento suficiente y se encuentra localizada en una zona de alto transito del personal (la cafetería), lo cual supone un riesgo, ya que se trata de elementos sensibles

	a ataques físicos intencionados o accidentales que se encuentran al alcance del personal interno y externo. Este plan pretende crear un nuevo espacio donde poder establecer un CPD, con las medidas de seguridad necesarias para asegurar el acceso solo al personal autorizado responsable, ofrecer unas condiciones adecuadas de temperatura y protección contra incendios, humedad y problemas eléctricos.
Subtareas	• Selección de una localización adecuada donde establecer el nuevo CPD. • Instalación de un armario en rack para situar los elementos de comunicaciones, los servidores, el NAS, el servidor de copias y los SAI pertinentes. • Instalación del cableado de red. • Realizar la instalación eléctrica adecuada, añadiendo sistemas de protección para impedir sobrevoltajes. • Climatización de la localización. • Sistema anti-incendio y anti-humedad. • Instalar un sistema de control de acceso.
Costes	Pendiente de presupuestar según proyecto.
Tiempo de ejecución:	3 meses
Riesgo residual:	El riesgo residual puede generarse cuando el sistema de acceso al CPD o los sistemas de climatización fallen durante un largo tiempo sin que nadie responda al evento. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la asociación.
Indicadores de eficacia y eficiencia:	Registro de los accesos del personal.

8.2.2. Programa de aseguramiento de la disponibilidad de los servidores

Tabla 151. Programa de seguridad – Aseguramiento disponibilidad servidores

ASEGURAMIENTO DISPONIBILIDAD SERVIDORES	**PRIORIDAD ALTA**
Objetivos:	• Implementar la alta disponibilidad en los servidores • Planificación de un Disaster Recovery de los servidores
Activos afectados:	HW009-Servidores, HW010- Servidores virtualizados
Participantes:	Gerencia y responsable TI
Salvaguarda:	[HW.A] Aseguramiento de la disponibilidad
Descripción:	El departamento TI es consciente de la importancia que tienen los servidores dentro del grupo empresarial, ya que desempeñan varias funciones importantes: - Ofrece los servicios del ERP, antivirus, dominio Windows, Active Directory, centralización de actualizaciones (WSUS), directivas de grupo (GPO), Wiki, el software propietario de la empresa, el software de control del inventario, DNS, servicio impresión, entre otros. - Es donde se almacena la información más valiosa y sensible. Además, cuenta con documentación compartida en los recursos compartidos entre los diferentes departamentos y toda la información del ERP, el programa de planificación e información de carácter personal. - Realizar tareas planificadas como copias de seguridad, actualizaciones... - Controlar el acceso de los usuarios del dominio a la red y a los diferentes recursos. El plan actual se basa en la creación de copias de seguridad y su restauración sobre una máquina de la que no se dispone en estos momentos, lo que supondría la parada de los servicios durante al menos dos días (el tiempo que se tardaría en comprar un nuevo servidor, montarlo, configurarlo y cargar una copia de seguridad). Por lo tanto, para implementar la salvaguarda [HW.A] Aseguramiento de la disponibilidad y reducir el riesgo que implica quedarse sin los servicios del servidor, se deberá de disponer de un par de nuevos servidores que ofrezcan apoyo al servidor principal y al servidor NAS

	Nota: Se recomienda que este plan se ejecute tras la conclusión del programa "CPD Dedicado" para poder instalar el nuevo servidor en su ubicación final.
Subtareas	• Analizar las opciones de las que se puede disponer para implementar la alta disponibilidad. • Comprar el hardware necesario. • Configurar el NAS secundario que actuará como espejo del principal. • Instalación de un servidor secundario con la estrategia **Pilot Light** (el servidor de respaldo duerme mientras el principal trabaja), en el que la información del servidor durmiente se vaya sincronizando cada poco tiempo con la información disponible en el servidor principal. • Instalar y configurar los sistemas para que actúen como secundarios. • Elaborar el plan de Disaster Recovery del servidor, como parte del plan de contingencia y recuperación del negocio. • Probar el procedimiento de Disaster Recovery Todos los registros, procedimientos y programas consisten en documentos legalizados y aprobados por el Departamento TIC y la administración de la organización.
Costes	Requiere un esfuerzo medio del departamento TIC, pero un importante gasto económico por parte de la administración. Aunque el plan se puede adaptar a las necesidades de administración. Para asegurar la disponibilidad de los activos de la empresa, necesitaremos el siguiente hardware y servicios externos: - Servidor NAS auxiliar = 600€ - Equipo servidor secundario = 1200€
Tiempo de ejecución:	2 meses para revisión de cumplimiento
Riesgo residual:	El riesgo residual puede generarse cuando tanto los servidores primarios como el secundario sufran daños catastróficos en el mismo instante. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la empresa.
Indicadores de eficacia y eficiencia:	Evaluar en los registros: errores, incidentes, como se responde ante una contingencia, daños y responsables. Planificar de forma periódica un simulacro de Disaster Recovery.

8.2.3. Programa de creación y formalización de las Políticas de Seguridad

Tabla 152. Programa de seguridad – Creación y formalización de las políticas de seguridad

CREACIÓN Y FORMALIZACIÓN DE LAS POLITICAS DE SEGURIDAD	PRIORIDAD ALTA
Objetivos:	• Creación y formalización de las políticas de seguridad
Activos afectados:	Todos los activos relacionados con el sistema de información del grupo empresarial deben tener asociadas políticas y procedimientos. Las políticas y procedimientos asociados dependerán del tipo de activo. Por lo tanto, se verán afectados todos los tipos de activos que se incluirán en las políticas de seguridad. [D] Datos / Información, [K] Claves criptográficas, [S] Servicios, [SW] Software – Aplicaciones informáticas, [HW] Equipamiento informático (hardware), [COM] Redes de comunicaciones, [MEDIA] Soportes de información, [AUX] Equipamiento auxiliar, [L] Instalaciones, [P] Personal.
Participantes:	Gerencia y responsable TI
Salvaguarda:	Política de Seguridad
Descripción:	En este programa de seguridad se abarcará la creación de las políticas, procedimientos y guías técnicas en materia de seguridad de la información. Actualmente, la empresa cuenta con ciertas normas y procedimientos no formalizados, por lo tanto se deberán de registrar y formalizar para que sea parte de la política de seguridad interna. La política de seguridad empresarial es el documento o documentos donde se recogen los objetivos de seguridad, se definen controles y se establecen directrices acordes a los requerimientos del negocio y de la normativa vigente. Una vez definidas las políticas, procedimientos y guías, estas serán distribuidas por toda la empresa para que estas políticas sean conocidas y aceptadas por los empleados.
Subtareas	• Creación de la Política de Seguridad del grupo empresarial. • Definición de los procesos de revisión, actualización y aprobación. • Elaboración de las políticas, procedimientos y guías. A continuación, se ofrece un ejemplo de aquellas que se consideran prioritarias:

	• Políticas: o Política de seguridad de la empresa: Objetivos de seguridad. o Política de copias de seguridad: Política para la realización de los backups. o Política de uso de Internet y correo electrónico: normativa del uso correcto. o Política de gestión de usuarios, grupos y perfiles, permisos, … o Política de gestión de claves: Claves de cifrado, certificados,… o Política de actualizaciones. o Política de acceso para el personal externo. o Política de respuesta ante los incidentes de seguridad. o Política de gestión de contraseñas: medidas de seguridad y uso de las contraseñas. o Política de antivirus: gestión, actualizaciones… o Código de uso aceptable: Normativa general de seguridad a cumplir por todos los empleados. o Política de cumplimiento de las normativas legales vigentes: Documentación de seguridad y manuales asociados. o Política de uso para los dispositivos de almacenamiento externo. o Política de confidencialidad de la información. • Procedimientos: o Procedimiento de altas/bajas de usuarios: gestión de los usuarios. o Procedimiento de cifrado de la información: criterios de cuándo y cómo cifrar la información. o Procedimiento de actuación del personal ante un corte del suministro eléctrico. o Procedimiento de actuación del personal ante una interrupción de un servicio. o Procedimientos de copias de seguridad: cómo hacer las copias. o Procedimiento de actuación ante la pérdida de un equipo: Pasos a realizar ante la pérdida de un equipo con información sensible. o Procedimiento de registro de incidentes: Información detallada acerca del incidente y su resolución. Se incluye la fecha/hora de

	la aparición del incidente, su tipo, la gravedad del incidente, los activos afectados, su posible origen, el estado actual del incidente, medidas tomadas para solventarlo, personal responsable y fecha hora de la resolución del incidente. • Guías técnicas: o Guía de configuración del correo. o Guía de configuración del ERP. o Guía de aseguramiento de la red. o Guía de securización de aplicaciones (navegador, correo, …) Todos los registros, procedimientos y programas consisten en documentos legalizados y aprobados por el Departamento TIC y la administración de la organización.
Costes	6 meses de trabajo de un especialista IT, para la elaboración de las políticas y documentación de soporte, la revisión junto al Responsable de Seguridad, más la difusión y explicación al resto de la empresa. Se considera el apoyo de la gerencia y los responsables de los diferentes departamentos, así como de la involucración del departamento legal.
Tiempo de ejecución:	6 meses para revisión de cumplimiento
Riesgo residual:	El riesgo residual puede generarse cuando algún empleado decida por su cuenta y riesgo incumplir las políticas. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la empresa.
Indicadores de eficacia y eficiencia:	Auditorias periódicas para comprobar el cumplimiento de las políticas. Registro y revisión de los incidentes de seguridad, con el objetivo de poder revisar la necesidad de reformas o creación de nuevas políticas.

8.2.4. Diseño e implementación de los perfiles de seguridad

Tabla 153. Programa de seguridad – Diseño e implementación de los perfiles de seguridad

DISEÑO E IMPLEMENTACION DE LOS PERFILES DE SEGURIDAD	PRIORIDAD ALTA
Objetivos:	• Identificar los accesos a los activos de la empresa. • Preservar la confidencialidad, integridad y autenticidad de la información
Activos afectados:	Los perfiles de seguridad afectaran a todos aquellos activos relacionados con la información, servicios, software, hardware y comunicaciones de la organización. Por lo tanto, incluiremos todos aquellos activos de forma agrupada. [D] Datos / Información, [K] Claves criptográficas, [S] Servicios, [SW] Software – Aplicaciones informáticas, [HW] Equipamiento informático (hardware), [COM] Redes de comunicaciones.
Participantes:	Gerencia y responsable TI
Salvaguarda:	[S.SC] Se aplican perfiles de seguridad [SW.SC] Se aplican perfiles de seguridad [HW.SC] Se aplican perfiles de seguridad [COM.SC] Se aplican perfiles de seguridad
Descripción:	Uno de los aspectos críticos dentro de la asociación es el riesgo que puede causar el acceso no autorizado a los datos. Por ello, se deben tomar medidas se seguridad para que los datos solo estén disponibles para los usuarios de los departamentos que correspondan. El primer punto es la gestión de empleados y usuarios, que para facilitar el trabajo del departamento TIC, será a través de grupos. Para clasificar a los grupos se puede considerar: departamento, lugar de trabajo, tipo de profesional, de acuerdo con la información y servicios que puede acceder, y en función de las acciones que puede ejecutar en el sistema e información. Definidos los grupos y a qué tienen acceso, se debe establecer el tipo de perfil que tendrán los usuarios de cada grupo. El perfil irá definido a través de la asignación de permisos de acciones sobre el sistema y la información a los

	que tienen acceso. Como norma general a los grupos se les debe asignar el mínimo privilegio y después cambiará conforme a los requerimientos. Para los usuarios se recomienda: elaborar un procedimiento de creación, modificación y borrado de cuentas, entregar de forma confidencial las credenciales de acceso, definir la caducidad de las contraseñas y definir procesos de bloqueos. Todas las actividades que se realicen cuando un empleado o usuario ingresa al sistema debe quedar registrado para evitar ataques de no repudio. Finalmente, periódicamente se debe realizar una revisión de las cuentas de usuarios, grupos, perfiles y los permisos que cada uno tiene. Esta revisión ayuda a no otorgar más permisos de los que se requiere y retirar otros servicios como correo electrónico y equipos informáticos a usuarios dados de baja.
Subtareas	• Revisar la creación de grupos y perfiles de empleados y usuarios. • Reestablecer, quitar u otorgar permisos a cada perfil o grupo. • Verificar el sistema de registros de actividades informáticas: logs. • Crear manuales para empleados, para el acceso a sistemas y aplicaciones así como para el uso de las contraseñas.
Costes	Requiere un esfuerzo alto del departamento TIC y la colaboración estrecha de la administración
Tiempo de ejecución:	2 meses para revisión de cumplimiento
Riesgo residual:	El riesgo residual puede generarse cuando a un empleado le sea entregado un perfil que no corresponde con su responsabilidad. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la asociación.
Indicadores de eficacia y eficiencia:	Revisar el cumplimiento del plan de seguridad a través de un checklist y verificando los registros de actividades

8.2.5. Formación y registro de procedimientos

Tabla 154. Programa de seguridad – Formación y registro de procedimientos

FORMACIÓN Y REGISTRO DE PROCEDIMIENTOS	PRIORIDAD MEDIA
Objetivos:	• Formar al personal, en el uso de las herramientas que se emplean en la empresa, para evitar que se comentan errores por el desconocimiento del uso de estas. • Registrar los procedimientos que se realizan para que puedan estar accesibles al personal para resolver cualquier duda o para que los nuevos empleados puedan usarlos como guía.
Activos afectados:	P001-Gerencia, P002-Oficina, P003-Comerciales
Participantes:	Gerencia y responsable TI
Salvaguarda:	[PS] Gestión del personal. [PS.AT] Formación y concienciación
Descripción:	La gran mayoría de incidentes que se producen con los datos en un entorno empresarial ocurren por descuidos o errores de los empleados, fruto del desconocimiento de las herramientas que se emplean en el día a día. Por lo tanto, es necesario educar a los empleados de la empresa acerca del uso correcto y óptimo de las herramientas y aplicaciones que se usan en el día a día en el entorno empresarial (ERP, software de gestión, cliente de correo electrónico, herramientas de diseño, etc.), por lo que se propone la realización de un curso a todos los empleados de la empresa y a los futuros empleados. Ya que la realización de los cursos no se puede realizar de forma continua, se propone también la generación de documentación y procedimientos de uso de las diversas herramientas, para que esta pueda servir de guía para resolver dudas puntuales o como material didáctico para nuevos empleados. La documentación podrá realizarse mediante la grabación audiovisual de los cursos y los procedimientos, que se podrá incorporar en una wiki destinada a los empleados de la organización.
Subtareas	• Concertación con un centro especializado de formación para la impartición de cursos de las diferentes herramientas (pueden también

	realizarse por el personal IT si se encuentran lo suficientemente familiarizados con las herramientas y procedimientos). • Realizar la documentación audiovisual o escrita del uso de las herramientas y de los procedimientos que sean de interés para la labor de los empleados. • Incorporar en la wiki los cursos y documentación, para que pueda ser visualizada de forma interna a la organización.
Costes	Curso de formación + h de asistencia responsable despacho + h de asistencia secretaria + h del responsable de generar la documentación.
Tiempo de ejecución:	6 meses para revisión de cumplimiento
Riesgo residual:	El riesgo residual puede generarse cuando un empleado no cumpla con este plan de seguridad. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la empresa.
Indicadores de eficacia y eficiencia:	Revisar el cumplimiento del plan de seguridad a través del descenso del número de errores cometidos por los empleados, para comprobar la respuesta.

8.2.6. Registro de la actividad informática

Tabla 155. Programa de seguridad – Registro de la actividad informática

REGISTRO DE LA ACTIVIDAD INFORMÁTICA	PRIORIDAD MEDIA
Objetivos:	• Establecer mecanismos para la monitorización de errores y amenazas. • Determinar eventos significativos dentro del sistema de la organización.
Activos afectados:	El registro de la actividad informática afectara a todos aquellos activos relacionados con la información, servicios, software, hardware y comunicaciones de la organización. Por lo tanto, los incluiremos de forma agrupada. [D] Datos / Información, [K] Claves criptográficas, [S] Servicios, [SW] Software – Aplicaciones informáticas, [HW] Equipamiento informático (hardware), [COM] Redes de comunicaciones.
Participantes:	Departamento TI
Salvaguarda:	[H.AU] Registro, auditoría, [H.tools.LA] Herramienta análisis logs, Registro incidentes de seguridad.
Descripción:	El uso de los servicios, aplicaciones, equipos y redes por parte de los usuarios genera actividad informática. El registro de toda esta información puede resultar de utilidad a la organización ayudando a la gestión y monitorización de los sistemas, permitiendo detectar incidentes y errores. Para el registro de toda esta actividad (incluyendo incidentes) se emplean los ficheros LOG. En muchos de estos sistemas los LOGs vienen desactivados por defecto, por lo que será necesaria activarlos y configurarlos para que nos permitan obtener información útil acerca de: • Cambios en las configuraciones. • Transacciones de importancia dentro de las aplicaciones. • Acceso y modificación de la información confidencial. • Modificación de permisos de acceso a red, aplicaciones o sistemas. • Inicio y fin de: conexión a red, ejecución de aplicaciones, sesiones de usuarios incluidos los intentos de sesión fallidos. • Límites de recursos de los equipos informáticos: capacidad de disco, memoria, ancho de banda, uso de CPU.

	• Inicio de actividad sospechosa detectada por antivirus y sistemas de detección de intrusos. Esta información se puede emplear para detectar fallos, errores, vulnerabilidades, comportamientos sospechosos, fines estadísticos y ataques. Por ello se debe establecer una política de gestión de LOGs y monitorización para generar alertas en tiempo real. Los registros deben incluir información tal como: identificador del usuario, identificador del recurso (fichero, servicio, aplicación, red, equipo, etc.), identificación del equipo dentro de la red, identificación de protocolos, fecha y hora de ocurrencia, y tipología del evento. Una vez configurados los LOGs, se requiere configurar un sistema de monitorización y registro que permitan darle valor a estos registros.
Subtareas	• Selección de los servicios, aplicaciones, equipos y redes que van a ser monitorizados. • Definir los formatos de los logs. • Seleccionar una solución para la monitorización de los logs. • Configuración y validación del sistema de monitorización. • Verificar el cumplimiento de registro de actividades informáticas. • Dar a conocer el plan de seguridad a toda la organización. • Definir un programa de revisión de cumplimiento del plan de seguridad.
Costes	Requiere un alto esfuerzo del departamento TIC. El coste de una solución de monitorización oscila entre 2000€ a 3500€, dependiendo de lo que se desee cubrir.
Tiempo de ejecución:	4 meses para tener el sistema en funcionamiento.
Riesgo residual:	El riesgo residual puede generarse cuando un empleado no cumpla con este plan de seguridad de logs o no se ha realizado correctamente. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la empresa.
Indicadores de eficacia y eficiencia:	Realizar pruebas controladas de incidentes y comprobar el funcionamiento del sistema de monitorización.

8.2.7. Copia de seguridad en la nube

Tabla 156. Programa de seguridad – Copia de seguridad en la nube

COPIA DE SEGURIDAD EN LA NUBE	PRIORIDAD MEDIA
Objetivos:	• Disponer de una copia de seguridad de la información de la organización bien protegida fuera de las instalaciones del grupo empresarial.
Activos afectados:	D005 - Copias de seguridad, SW009 - Sistema de backup
Participantes:	Gerencia y responsable TI
Salvaguarda:	[SW.A] Copias de seguridad (backup) [D.A] Copias de seguridad de los datos (backup)
Descripción:	Dentro de la estrategia de TI de la empresa de mover servicios a la nube, una de las líneas de trabajo sería evaluar el hospedaje de las copias de seguridad en la nube. Actualmente, todas las copias de seguridad que se realizan de la organización se almacenan en las propias instalaciones de la empresa, por lo que en el caso de una catástrofe en las instalaciones se podrían perder los activos de la información junto a sus copias de seguridad. Por lo tanto, en este plan se considera realizar un análisis de los posibles servicios de almacenamiento en la nube existentes, para encontrar uno que ofrezca las siguientes garantías de seguridad a un precio que sea atractivo para la gerencia. El hecho de utilizar este servicio desde la nube supondría "compartir" el riesgo con el proveedor en materia de seguridad y alta disponibilidad de las copias de seguridad. Tras la selección y evaluación del servicio de hosting en la nube, se presentara la propuesta a gerencia para ser evaluado. En el caso de ser aceptado, se procederá a automatizar el envío de las copias de seguridad a la nube tan pronto como se realicen. En caso, contrario se buscaran alternativas.
Subtareas	• Realizar el análisis del servicio de almacenamiento en la nube. • Configurar copia de seguridad ERP en la nube.

Costes	1 empleado del departamento TIC para realizar el análisis y selección de cloud. 50-100 euros por el servicio cloud al año.
Tiempo de ejecución:	1 mes para análisis, evaluación, selección de backups a hospedar en cloud.
Riesgo residual:	El riesgo residual puede generarse cuando el responsable no proteja adecuadamente las credenciales de acceso a la nube. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la empresa. Se trata de un riesgo compartido entre la organización y el proveedor del servicio cloud.
Indicadores de eficacia y eficiencia:	Revisar el funcionamiento del servicio de cloud, para comprobar la respuesta.

8.2.8. Control de acceso

Tabla 157. Programa de seguridad – Control de acceso

CONTROL DE ACCESO	PRIORIDAD MEDIA
Objetivos:	• Identificar los accesos físicos a las instalaciones. • Proteger el acceso a los activos. • Preservar la confidencialidad de la información
Activos afectados:	El control de acceso físico permitirá proteger todos los activos de los que dispone la organización. [D] Datos / Información, [K] Claves criptográficas, [S] Servicios, [SW] Software – Aplicaciones informáticas, [HW] Equipamiento informático (hardware), [COM] Redes de comunicaciones, [MEDIA] Soportes de información, [AUX] Equipamiento auxiliar, [L] Instalaciones, [P] Personal.
Participantes:	Todos los departamentos de la empresa
Salvaguarda:	[L.AC] Control de los accesos físicos [PS.AT] Formación y concienciación
Descripción:	El riesgo que puede causar el acceso no autorizado a las instalaciones, es de los riesgos más críticos que se pueden dar en la empresa. Para proteger el acceso físico a los activos y proteger la confidencialidad de la información, el plan de control de acceso considera: • Lo primero que se debe controlar es el acceso físico a las Instalaciones. Todos los edificios deben poseer seguridad en todos sus accesos para cuando las actividades diarias culminen. Seguridad extra deben tener oficinas de administradores, el departamento TIC y todos los cuartos en los que se encuentren equipos informáticos, soportes de información o activos críticos para la asociación. La protección puede ser con llaves, acceso electrónico y cámaras de seguridad. • En todas las instalaciones deberán registrarse las personas que accedan y cuál es su motivo. Por ello, se deben dar credenciales a los empleados y usuarios para facilitar el acceso a quien ya tiene permiso. Las personas externas obligatoriamente realizarán un registro en la recepción.

	• Para evitar accesos no autorizados, es esencial la señalización de aquellas zonas en las que se prohíbe el ingreso, especialmente de equipos informáticos. • Para los lugares, cuartos, ubicaciones o armarios en donde se encuentren dispositivos informáticos se debe crear registros de quién accede, a la hora que lo hace y cuál será la acción que realiza. Este procedimiento ayuda a evitar ataques o el repudio de acciones. • Para almacenar llaves de cuartos, armarios o seguros de los equipos informáticos serán almacenadas en una caja fuerte a la que tengan acceso solo personal del departamento TIC. • Se crearán manuales de uso correcto de las instalaciones que contengan equipos informáticos para los empleados de limpieza. De igual manera todos los laboratorios informáticos deberán poseer un informativo de normas y buenas prácticas.
Subtareas	• Crear los registros para personal externo. • Entregar credenciales a empleados y usuarios de uso obligatorio. • Verificar la señalización de las instalaciones especialmente en las ubicaciones de equipos informáticos. • Guardar todas las llaves de acceso a equipos informáticos. • Crear manuales de uso y buenas prácticas para las instalaciones críticas. Todos los registros, procedimientos y programas consisten en documentos legalizados y aprobados por el Departamento TIC y la administración de la organización.
Costes	Requiere un esfuerzo alto del departamento TIC y la administración.
Tiempo de ejecución:	2 meses para revisión de cumplimiento
Riesgo residual:	El riesgo residual puede generarse cuando un intruso logre acceder a las instalaciones con intenciones perjudiciales para la empresa. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la empresa.
Indicadores de eficacia y eficiencia:	Evaluar en los registros: errores, incidentes, como se responde ante una contingencia, daños y responsables.

8.2.9. Plan de actuación frente a imprevistos

Tabla 158. Programa de seguridad –Plan de actuación frente a imprevistos

PLAN DE ACTUACIÓN FRENTE A IMPREVISTOS	PRIORIDAD MEDIA
Objetivos:	• Elaboración de un plan de contingencia y recuperación ante incidentes. • Definir el método de actuación para minimizar el impacto de las posibles amenazas que afecten a la empresa.
Activos afectados:	Los planes de contingencia y recuperación afectaran todos los activos de los que dispone la organización. [D] Datos / Información, [K] Claves criptográficas, [S] Servicios, [SW] Software – Aplicaciones informáticas, [HW] Equipamiento informático (hardware), [COM] Redes de comunicaciones, [MEDIA] Soportes de información, [AUX] Equipamiento auxiliar, [L] Instalaciones, [P] Personal.
Participantes:	Gerencia y responsable TI
Salvaguarda:	[BC] Continuidad del negocio [BC.DRP] Plan de Recuperación de Desastres (DRP)
Descripción:	Teniendo en cuenta que un sistema nunca va a estar 100% protegido es importantes definir la estrategia a seguir en caso de que se produzca una incidencia grave para intentar que cause el menor impacto posible. Para ello, se desarrollará una serie de planes de contingencia y continuidad en los cuales se organizará el personal del centro en equipos, se establecerán funciones y responsabilidades en caso de incidencia, se definirán los procedimientos de actuación y la estrategia para la vuelta a la normalidad. La creación de equipos es importante para que, en caso de incidencia, una parte de personal se encargue de atender esa incidencia mientras que el resto del personal se dedica a su actividad habitual. En el capítulo 9.1 definiremos la estructura que deben seguir los planes de contingencia y continuidad. Además, se creara uno para que sirva de ejemplo para que sirva de ejemplo para el diseño del resto.
Subtareas	• Organizar el personal del centro en equipos. • Evaluar posibles casos de incidentes. • Generar protocolos de actuación por equipos acorde a los incidentes.

	• Establecer simulacros para poner a prueba los protocolos establecidos y evaluar su eficacia. Todos los registros, procedimientos y programas consisten en documentos legalizados y aprobados por el Departamento TIC y la administración de la organización.
Costes	Requiere un esfuerzo alto del departamento TIC. Dependerá del salario de los trabajadores del departamento TIC y de administración.
Tiempo de ejecución:	5 meses para revisión de cumplimiento
Riesgo residual:	El riesgo residual puede generarse cuando un caso no está valorado en el plan de contingencia y continuidad. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la empresa.
Indicadores de eficacia y eficiencia:	Evaluar en los registros: errores, incidentes, como se responde ante una contingencia, daños y responsables.

8.2.10. Programas adicionales para futuras revisiones

Al contar ya con un número de planes prioritarios, los planes considerados de prioridad baja se aportan para ser considerados en las futuras revisiones del Plan Director de Seguridad. Por lo tanto, serán nombrados y descritos de forma breve.

- **Programa de actualizaciones y mantenimiento**: en este programa se establecerán las políticas de actualizaciones que deben seguirse para mantener las aplicaciones, los sistemas y el hardware correctamente actualizados. Además, se deberá considerar que cuando se requiera actualizar una aplicación se deberá de revisar el tipo de actualización, y determinar si es o no necesario realizar el cambio.
- **Cifrado de los datos esenciales**: actualmente solo se cifran las copias de seguridad de los datos más importantes, pero sería muy beneficioso para la organización que se comenzasen a cifrar la información más sensible para que solo aquellos con los credenciales adecuados pudiesen acceder a ellos.
- **Programa de migración de contraseñas al uso de certificados**: en este programa se establecerán las medidas para configurar el uso de certificados para establecer las conexiones a los servicios de la empresa y para el uso de la VPN.
- **Programa para la monitorización del tráfico de red**: en este programa se considera la instalación y configuración de una herramienta que permita a la administración la monitorización del tráfico de datos interno de la organización, permitiendo a los administradores observar abusos o irregularidades que puedan suceder en la red.
- **Programa de chequeo de configuraciones**: en este programa se propone la instalación y configuración de una herramienta de chequeo de las configuraciones para ayudar a los administradores a no cometer errores en la configuración de los servicios y el software.
- **Programa periódico de auditoria de seguridad**: este programa incluirá la realización de auditorías de sistemas y seguridad de forma periódica. Se puedo incluir el análisis de vulnerabilidades de los sistemas a través de pruebas de pentesting.
- **Configuración del entorno de prueba para el desarrollo**: en este programa se considera la configuración de un entorno de pruebas debidamente adecuado, con el objetivo de que los desarrollos internos de la empresa se encuentren correctamente aislados y evitar así que errores de los desarrolladores se extiendan a los sistemas de la organización.

8.3. El Plan Director de la empresa

Una vez definidos los programas de seguridad es necesario organizarlos en un plan de seguridad también llamado plan director.

Un plan director se centra, generalmente, en un plazo de tiempo de unos 2 o 3 años y define los programas de seguridad y las medidas a tomar en ese plazo. El objetivo es definir en ese periodo de tiempo como se van a organizar los programas de seguridad propuestos en el apartado anterior. Para ello se tendrá en cuenta la duración y el coste de los programas, la urgencia de implantación (teniendo en cuenta si el riesgo que buscan mitigar es más o menos crítico), la capacidad del personal…

Se ha estructurado el plan de seguridad de forma que los primeros proyectos estén enfocados a los activos con mayor riesgo y posponiendo los programas con mayor coste para que el centro tenga capacidad para ahorrar ese dinero.

Así, el plan director estructura los proyectos a realizar de la siguiente forma, con la estimación de conclusión en dos años:

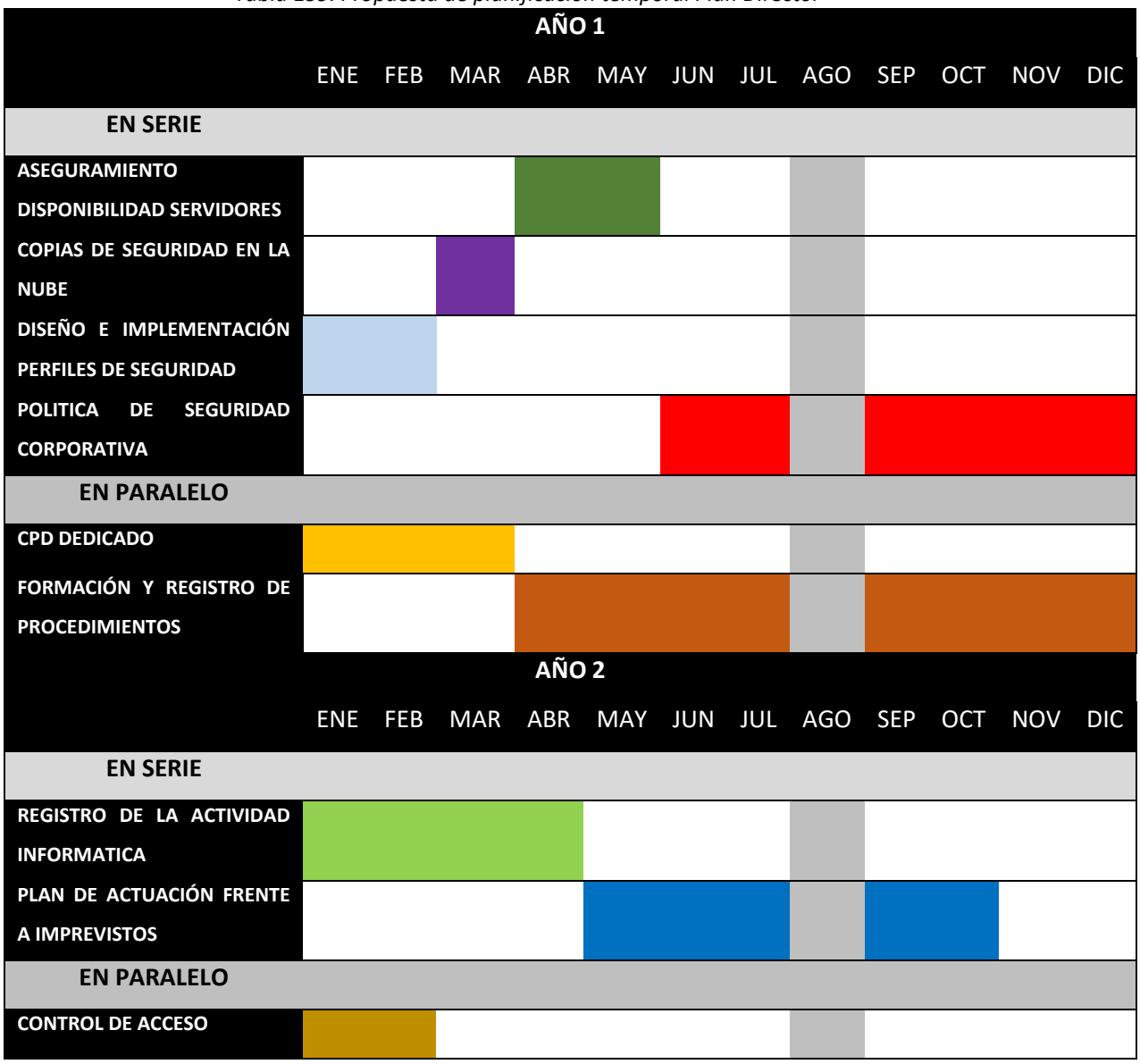
Planes de desarrollo secuencial por el departamento de TIC

- ASEGURAMIENTO DE LA DISPONIBILIDAD SERVIDORES. 2 meses
- DISEÑO E IMPLEMENTACIÓN DE LOS PERFILES DE SEGURIDAD. 2 meses
- CREACIÓN Y FORMALIZACION DE LAS POLITICAS DE SEGURIDAD. 6 meses
- COPIA DE SEGURIDAD EN LA NUBE. 1 mes
- REGISTRO DE LA ACTIVIDAD INFORMATICA. 4 meses
- PLAN DE ACTUACIÓN FRENTE A IMPREVISTOS. 5 meses

Planes de desarrollo en paralelo por el departamento de TIC

- CDP DEDICADO. 3 meses
- PLAN DE FORMACIÓN Y REGISTRO DE PROCEDIMIENTOS. 6 meses
- CONTROL DE ACCESO. 2 meses

Tabla 159. Propuesta de planificación temporal Plan Director



9. Planes de contingencia

Tal y como se explica en el punto 4.6 “Plan de contingencia y continuidad de negocio” del capítulo 4 “Estado del Arte”, el Plan Director de Seguridad se debe completar con otros elementos que permitan a la organización recuperarse de un desastre a la vez que le permita mantener la continuidad del negocio. Aquí entran en juego los Planes de contingencias y continuidad de negocio.

Una buena planificación de recuperación de la actividad normal por parte de una empresa ante un desastre permitirá minimizar el impacto económico que pueda ocasionar la materialización de la amenaza, evitar la fuga o robo de información crítica, evitar problemas legales y repercutirá favorablemente a la imagen y reputación de la empresa.

Por lo tanto, en este capítulo nombraremos los planes de contingencia y recuperación que se creen oportunos y prioritarios para el grupo empresarial en el que este TFM basa su estudio. Como el desarrollo de cada uno de los planes de contingencia podría abordar bastante trabajo, simplemente realizaremos el desarrollo de uno de ellos, para que pueda servir como ejemplo para desarrollar el resto de ellos.

9.1. Planes de contingencia y continuidad de negocio.

Tras estudiar las amenazas más probables, se establecen los siguientes planes de contingencia y continuidad para afrontar situaciones en las que se han materializado las amenazas.

- Proceso de la gestión de la producción ante la amenaza de pérdida del servidor.
- Proceso de la gestión empresarial ante la amenaza de pérdida de la conexión a Internet.
- Proceso de la gestión empresarial ante la amenaza de infección de uno o varios equipos de virus o la propagación de un ransomware.
- Proceso de la gestión empresarial ante la detección de una intrusión externa.
- Proceso de la gestión empresarial ante la amenaza de fallo eléctrico grave en el CPD.

9.2. Plan de contingencia y continuidad de negocio para el proceso de "Gestión de la producción" ante la amenaza de pérdida del servidor.

El objetivo será realizar un plan de contingencia para el proceso de "Gestión de la producción", ante la amenaza de pérdida del servidor. Para ello, describiremos las fases que se deben seguir para que el negocio se vea afectado lo menos posible y para que pueda retornar a un estado óptimo.

9.2.1. Fase 0: Determinar el alcance

En este plan de continuidad vamos a abordar un enfoque por procesos. Por lo tanto, vamos a tomar el proceso de gestionar la producción de la empresa, el cual engloba una serie de acciones y es prácticamente, el proceso más importante para el funcionamiento correcto del grupo empresarial en la que estamos basando el proyecto.

Ante un desastre en los servidores de la empresa, la gestión de la producción ser verá afectada y con ella los siguientes activos de la empresa:

- **Empleados del departamento de producción**. El trabajo del personal de producción se ve comprometido.
- **Operarios**. El trabajo de los operarios se ve comprometido.
- **ERP Corporativo**. Al no disponer de acceso al ERP Corporativo no se puede comprobar el estado de los proyectos, ni asignar tareas, ni registrar datos acerca de los procesos de fabricación.
- **Documentación y planos producción**. Al no disponer de acceso a la documentación ni a los planos de los productos a fabricar, no se puede fabricar nada.
- **Tabletas producción**. Al no disponer de acceso a los datos, no se puede registrar ninguna tarea de producción.

Este desastre, puede afectar además a otros procesos definidos en el análisis de impacto en el negocio (BIA), tal como el cálculo de costes de los productos, el proceso de compra/venta y la gestión de los proyectos.

9.2.2. Fase 1: Análisis de la organización

Ahora que conocemos la organización y el proceso en el que deseamos establecer el plan de continuidad y recuperación, el siguiente paso es realizar un análisis formal sobre el Negocio o BIA (Business Impact Analysis).

Análisis del Impacto sobre el Negocio.

En este apartado vamos a definir los requisitos temporales y de recursos de los procesos dentro del alcance y, junto con el Análisis de Riegos definiremos las iniciativas a implantar para recuperar los procesos en situación de contingencia. Para el proceso "Gestión de la producción" determinaremos los siguientes datos:

- **Tiempo de recuperación (RTO - Recovery Time Objetive).**

  Para obtener el tiempo de recuperación vamos a sumar los tres tiempos en los que este se divide:

  - **Tiempo de detección**: La detección de este problema durante horario de trabajo será inmediata, ya que, los programas de los que depende la empresa dejaran de funcionar y enseguida se darán cuenta de que hay algún problema con el servidor. Fuera del horario de oficina (7-15), existen 2 turnos más en los que trabajan los operarios (tarde y noche), por lo que en ese caso, serán los responsables de producción los que darán la voz de alarma y avisarán al responsable de informática (entre 5 y 10 minutos). En domingos o días festivos, no se realizará ningún aviso.
  - **Tiempo de toma de decisiones**: En analizar el problema y comprobar su alcance, se suele tardar entre 15-30 minutos dependiendo si es necesario avisar a gerencia sobre el problema o no.
  - **Tiempo de reparación del problema**: Dependiendo si es un problema de rápida subsanación o no, el tiempo de reparación puede llevar desde media hora para reparaciones sencillas (configuración, cambiar alguna pieza común como fuente de alimentación), a 48 horas para preparar, configurar y levantar otra máquina que haga el papel del servidor de forma temporal en el que se cargaran las copias de seguridad.

  Por lo tanto, el tiempo de recuperación aproximado dependiendo del daño sufrido por el servidor, puede ser de 1 hora a 48 horas.

- **Recursos humanos y tecnológicos**

  En el proceso de recuperación ante estos incidentes, actúan los siguientes recursos humanos:

  - **Departamento de informática**: Son los encargados de investigar y solucionar el problema, ya sea software o hardware.
  - **Departamento de gerencia**: Solo participa si se requiere algún tipo de inversión temporal comprando nuevo hardware o contratando algún servicio externo.

  En cuanto a los recursos tecnológicos utilizados nos encontramos con los siguientes:

  - **Servidor de reserva**: Equipamiento informático de reserva que tras configurarlo puede actuar como servidor.
  - **Sistemas externos de almacenamiento** en los cuales se realizan las copias de seguridad periódicas de los datos de la empresa.

- **Tiempo máximo tolerable de caída (MTD - Maximum Tolerable Downtime).**

  Este tiempo puede variar dependiendo de la carga de trabajo en la producción. Pero por lo general, a partir de las 8 horas sin solucionar el problema, podemos encontrarnos con serias consecuencias para la empresa, que pueden acarrear pérdidas económicas y de reputación.

- **Niveles mínimos de recuperación del servicio (ROL - Revised Operating Level).**

  Un nivel mínimo de recuperación del servicio, podría considerarse teniendo de nuevo el servicio ERP levantado y funcionando con los datos de la última copia de seguridad realizada antes de la ocurrencia del desastre. Poco a poco, deberán irse añadiendo el resto de servicios y conexiones con el resto de información de la empresa.

- **Dependencia de otros procesos internos o proveedores.**

  En el caso de que sea un problema hardware, se dependerá del proveedor de equipamientos informáticos para que envíe cuanto antes un equipo de repuesto que poder usar como servidor temporal.

- **Grado de dependencia de la actualidad de los datos (RPO - Recovery Point Objective).**

  Se realizan backups cada 8 horas, así pues, enfrentarnos a este problema supondría la pérdida del trabajo realizado por los empleados de todos los departamentos. Por tanto,

el máximo de trabajo que podemos llegar a perder es del realizado en 8 horas, esto en proyectos donde la fecha de entrega es muy cercana puede resultar fatal y puede conllevar una pérdida económica y de credibilidad de la empresa.

Análisis de los riesgos.

El análisis de los riesgos ya se ha realizado en anteriores apartados, por lo tanto, en este vamos a utilizar este trabajo realizado para ver cuáles son los activos críticos que están involucrados en el proceso.

En el proceso de Gestión de la Producción podemos ver que el activo principal de este proceso es el Servidor, así pues vamos a comprobar que amenazas vamos a abordar en este plan de continuidad.

En total, encontramos 21 amenazas que pueden afectar al servidor, pero hemos resumido la lista en las amenazas que más afectarían al activo y por lo tanto al proceso si ocurriesen.

Tabla 160. Amenazas con mayor riesgo en el servidor

Amenaza	Integridad	Confidencialidad	Disponibilidad
[I.1] Fuego			**RIESGO GRAVE**
[I.2] Daños por agua			**RIESGO GRAVE**
[I.5] Avería de origen físico o lógico			**RIESGO GRAVE**
[A.6] Abuso de privilegios de acceso		**RIESGO GRAVE**	
[A.25] Robo		**RIESGO GRAVE**	**RIESGO GRAVE**

En este plan de continuidad vamos a abordar la amenaza de Avería de origen lógico o físico, ya que es una de las amenazas que más probabilidades tiene de ocurrir.

Las medidas a tomar para esta amenaza serán la de mitigarla con salvaguardas tales como:

- Copias de seguridad (backup).
- Aseguramiento de la disponibilidad.
- Control de acceso físico y lógico.
- CPD Dedicado.

A pesar de estas medidas, no hay riesgo cero, por ello vamos a determinar en las siguientes fases el plan de continuidad ante la ocurrencia de la amenaza.

9.2.3. Fase 2: Determinación de la estrategia de continuidad

Ante este tipo de amenazas, tenemos un plan de continuidad que consta de una opción principal y una segunda opción que se llevaría a cabo en caso de que la primera fallase o no se dispongan de los recursos necesarios en el momento.

La primera opción consiste en tener un segundo servidor de respaldo con una estrategia **Pilot Light** (el servidor de respaldo duerme mientras el principal trabaja), en el que la información del servidor durmiente se vaya sincronizando cada poco tiempo con la información disponible en el servidor principal.

Esto sería realizado por el departamento de informática, supervisado por el departamento de gerencia para asegurar que el servidor cumple con los requisitos técnicos que el departamento de informática demande.

En esta opción, el RTO sería prácticamente inmediato, ya que simplemente se trataría de cambiar las configuraciones de los programas para que empleen el servidor secundario como nuevo servidor principal. En cuanto al RPO, tendríamos una pérdida de datos de solo algunas horas, ya que el servidor secundario durmiente cada pocas horas realizara una copia incremental de la información.

Incluso podría considerarse algún tipo de script, que despierte al servidor durmiente y lo configure como nuevo servidor de forma automática, al detectar el servidor principal como caído.

Esta opción es considerada como primaria, ya que la empresa desea mantener la confidencialidad de sus datos de forma interna en la empresa y no confía de los servicios en la nube.

La segunda opción consiste en tener un equipo virtualizado en la nube que pueda activarse cuando sea requerido para actuar como lo hacía el servidor principal. Al contrario que la primera opción, esta opción **no emplearía la estrategia Pilot Light** (el servidor de respaldo duerme mientras el principal trabaja). En este caso, será necesario arrancar el sistema, cargar las ultimas copias de seguridad y configurar los programas para que apunten al servidor en la nube.

Esto sería realizado por el departamento de informática, supervisado por el departamento de gerencia para asegurar que el servicio en la nube cumple con los parámetros de confidencialidad y seguridad que la gerencia desea sobre los datos.

En esta opción, el RTO sería aproximadamente de 4 horas, ya que se trataría de cargar las copias de seguridad y cambiar las configuraciones de los programas para que empleen el servidor secundario como nuevo servidor principal. En cuanto al RPO, dependería de la configuración de las copias de seguridad, actualmente se realizan tres copias diarias.

Esta opción supondría un coste económico menor, ya que solo se encendería en el caso de que fuese necesario.

9.2.4. Fase 3: Respuesta a la contingencia

En respuesta a la amenaza de Avería de origen físico o lógico en el Servidor, seguiremos el procedimiento expuesto en la fase anterior, cuyos pasos se explicarán en la presente fase siguiendo este plan de crisis.

Plan de crisis.

Este documento tiene como objetivo gestionar los momentos iniciales de la crisis, para ello definiremos los siguientes puntos:

- **Condiciones de disparo:** Los programas que dependen del servidor dejan de funcionar.
- **Flujos de toma de decisiones:** El responsable del departamento de informática debe comunicar a Gerencia el incidente y decidir si se requiere una recuperación inmediata o no.
- **Medios para la declaración de la situación de crisis:** El responsable de Gerencia envía un correo electrónico circular avisando del problema al resto de departamentos y propone registrar en papel todas aquellas actividades que se vayan realizando, para más tarde registrarlo donde se deba.
- **Personal responsable de la situación de crisis:** Departamento de informática.
- **Datos de contacto de los responsables de gestionar la crisis:** Utilizar el teléfono con el número de marcación rápida para contactar con el responsable del departamento de informática.
- **Niveles de priorización de recuperación de la infraestructura:** El objetivo principal es poner de nuevo en marcha el servicio de ERP y cargar los datos más actualizados. A continuación, se irán levantando el resto de servicios necesarios para la Gestión de la Producción.
- **Requisitos temporales de puesta en marcha:** Aproximadamente de 1 hora a 4 para volver a recuperar la actividad.

- **Planes operativos y personal responsable:** Se disponen de dos planes: servidor de respaldo Pilot Light local y en caso de que este no pueda llevarse a cabo, un segundo plan empleando un servidor en la nube en el cargar manualmente los backups. El personal responsable en ambos casos será el departamento de informática.

Tabla 161. Plan de crisis de la respuesta a la contingencia

Paso	Tiempo	Acción	Información adicional	Personal
1	0 m	Identificación de la condición que provoca la situación de crisis.	Los programas que dependen del servidor dejaran de funcionar	Operarios. Empleados departamentos.
2	5 m	Avisar el departamento de informática	Teléfono: marcación rápida	Responsable departamento
3	10 m	Informar al departamento de gestión de la situación de crisis actual	Teléfono: marcación rápida	Responsable departamento informática
4	15 m	Avisar a todos los empleados del incidente	Envío de un correo electrónico de alta prioridad	Gerencia
5	15 m	Comenzar a apuntar todas las acciones, cantidades y horas en papel, empleando las plantillas disponibles para el tipo de acción.		Operarios. Empleados departamentos.
6	15 m	Ejecutar el plan Operativo de Recuperación de entorno.	En caso de que el primer plan no funcione, ejecutar el segundo plan.	Departamento informática
7	75-135 m	Informar al departamento de gestión del restablecimiento del sistema y vuelta al funcionamiento normal	Teléfono: marcación rápida	Responsable departamento informática
8	140 m	Avisar a todos los empleados de la resolución del incidente	Envío de un correo electrónico de alta prioridad	Gerencia
9	140 m	Fin del plan de crisis		

Plan Operativo de Recuperación de Entornos y procedimientos técnicos de trabajo.

En este documento se detallan los pasos a seguir por los responsables de informática para restablecer los sistemas:

PLAN A: Sustituir el servidor por el servidor de respaldo

Tabla 162. Plan A. Sustitución del servidor por uno de respaldo

Paso	Tiempo	Acción	Información adicional	Personal
1	0 m	Comprobaciones básicas para comprobar el no funcionamiento del servidor		Responsable departamento informática
2	5 m	Despertar el servidor dormido y asignarlo como principal		Departamento informática
3	15 m	Modificar las configuraciones para redirigir las conexiones a la maquina sustituta		Departamento informática
4	25 m	Comprobar la fecha y hora de los datos, para avisar del tiempo de trabajo del que no se disponen datos.	Envío de un correo electrónico a gerencia con el aviso	Departamento informática
5	30 m	Comenzar las reparaciones en el servidor caído.		Departamento informática
7	30 m	Informar al departamento de gestión del restablecimiento del sistema y vuelta al funcionamiento normal	Teléfono: marcación rápida	Departamento informática
8	30 m	Fin del plan A		

PLAN B: Sustituir el servidor caído por un servidor temporal en la nube

En el caso de que el plan A falle por alguna razón (ya sea física o lógica), llevar a cabo el plan B.

Tabla 163. Plan B. Sustituir el servidor por servicios en la nube

Paso	Tiempo	Acción	Información adicional	Personal
1	0 m	Comprobaciones básicas para comprobar el no funcionamiento del servidor.		Responsable departamento informática
2	5 m	Acceder a la web/aplicación del servicio externo que activará el servidor en la nube.	Utilizar las credenciales responsabilidad del responsable.	Responsable departamento informática

3	15 m	Arrancar el servidor pre-configurado con los servicios de la empresa.	Es necesario tener los servicios actualizados tal y como se encuentran en el servidor original. En caso contrario, el proceso se alargará bastante.	Departamento informática
4	30 m	Obtener los backups de los medios de almacenamiento externos	Los medios de almacenamiento se guardan bajo llave.	Departamento informática
5	40 m	Cargar los últimos backups disponibles antes del incidente en los servicios en la nube	Dependiendo de la conexión de la red.	Departamento informática
6	100 m	Modificar las configuraciones para redirigir las conexiones a la maquina en la nube		Departamento informática
7	110 m	Comprobar la fecha y hora de los datos, para avisar del tiempo de trabajo del que no se disponen datos.	Envío de un correo electrónico a gerencia con el aviso.	Departamento informática
8	120 m	Comenzar las reparaciones en el servidor caído.		Departamento informática
9	120 m	Informar al departamento de gestión del restablecimiento del sistema y vuelta al funcionamiento normal	Teléfono: marcación rápida	Departamento informática
10	120 m	Fin del plan B		

Una vez la crisis ha sido estabilizada, será necesario realizar una traza para la recuperación de entornos, es decir, será necesario hacer un estudio de los puntos siguientes:

- Determinar que activos se han visto afectados por la crisis y tratar de repararlos.
- Determinar la magnitud de la crisis.
- Intentar determinar el por qué ha ocurrido esta crisis.

9.2.5. Fase 4: Pruebas, mantenimiento y revisión.

Con el afán de que los procedimientos anteriormente explicados se encuentren actualizados y funcionales ante cualquier tipo de cambio, será necesario realizar un plan de pruebas y mantenimiento.

Plan de mantenimiento.

Las tareas de mantenimiento se encargarán de mantener actualizada la infraestructura de reserva y la documentación cuando el servidor principal sufra algún cambio (ya sea en su funcionamiento por medio de una actualización, un cambio de sus políticas o acuerdos legales, etc.) se procurará que las opciones presentadas en la anterior fase cambien si es necesario. Dependiendo de cada plan tendremos:

- **Plan A**: En cuanto al mantenimiento del servidor de reserva en local, se requiere que se revise con cierta regularidad (cada semana) su correcto funcionamiento. Además, cada vez que se realice algún cambio o actualización en el servidor principal, también será necesario replicarlo en el de reserva para mantener la sincronía de aplicaciones y sus versiones.
- **Plan B**: El mantenimiento será el mismo que en el caso del Plan A, pero además tendremos que tener en cuenta los posibles cambios en las configuraciones o políticas de la empresa externa que nos ofrece el servicio, para en caso necesario, actualizar el servidor principal a las exigencias del servicio. Como por ejemplo, una actualización del sistema operativo.

Plan de pruebas.

Las tareas de pruebas se encargarán de comprobar que las opciones que tenemos para recuperar los datos funcionan como es debido y los pasos que hemos definido en las opciones de recuperación son correctas. En este caso, los planes de prueba se ejecutarán de 2 a 4 veces por año (dependiendo de la antigüedad del servidor principal y la posibilidad que tenga de fallar), en un fin de semana o día en los que no haya apenas carga de trabajo, como los días antes de las vacaciones de verano o navidad. Dependiendo de cada plan tendremos:

- **Plan A**: Para ejecutar la prueba se desconectará el servidor de la red y esperaremos a que los empleados den la voz de alarma y sigan el procedimiento de acuerdo a lo establecido, tras ello, el departamento de informática procederá a reemplazarlo por el servidor durmiente, comprobando el tiempo que se tarda en el proceso y comprobar

que los pasos creados para recuperar el sistema son los mismos. En caso de que no lo fuesen será necesario que se redefina la estrategia de recuperación de datos de este método de forma inmediata, y se realice un estudio de por qué realizando las tareas de mantenimiento no se ha notificado en un cambio en el proceder del plan de crisis.

- **Plan B**: Para ejecutar la prueba se realizará lo mismo que en el caso del Plan A, pero en este caso se utilizarán los servicios de servidor virtualizado de una empresa externa, para evaluar que los parámetros ofrecidos por la empresa externa se corresponden a lo contratado. De igual forma, si se detecta que con las instrucciones dadas en el plan de crisis para la segunda opción, no se alcanza a la solución deseada, se realizará una investigación del por qué.

10. Planes de concienciación

En este punto, diseñaremos un plan de concienciación dirigido a ofrecer una formación general del personal en materia de ciberseguridad. Para ello, y basándonos en el análisis y los resultados previos, diseñaremos una acción en la cual se realice primero un ataque dirigido para crear alarma controlada, y después una formación específica mediante algún seminario, curso, folleto o tríptico que ilustre sobre la ciberseguridad.

El grupo empresarial en el que estamos basando el proyecto es una empresa con un perfil bajo sobre tecnologías de la información, por lo que la campaña a diseñar ira orientada a usuarios de nivel medio/bajo en las tecnologías de la información.

Para diseñar la campaña, tendremos que seguir una serie de puntos que nos permitirán demostrar personalmente los problemas que podría ocasionar en fallo de seguridad y como se puede actuar para que no vuelva a repetirse.

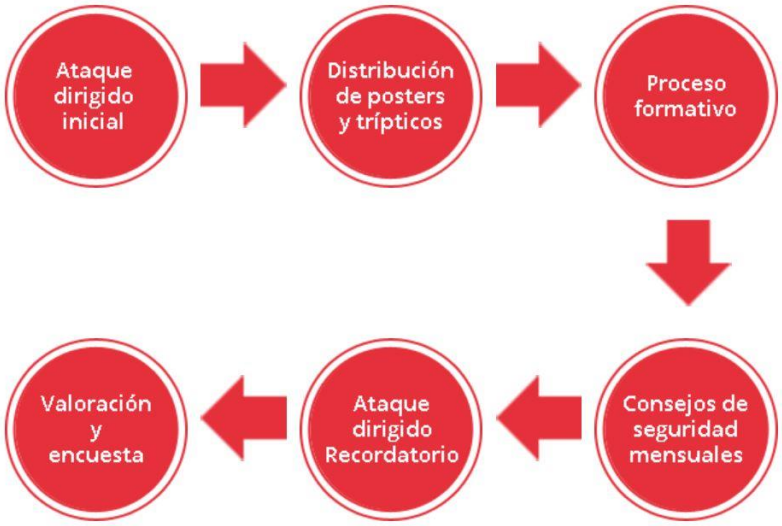


Figura 10. Fases de la campaña de concienciación [15]

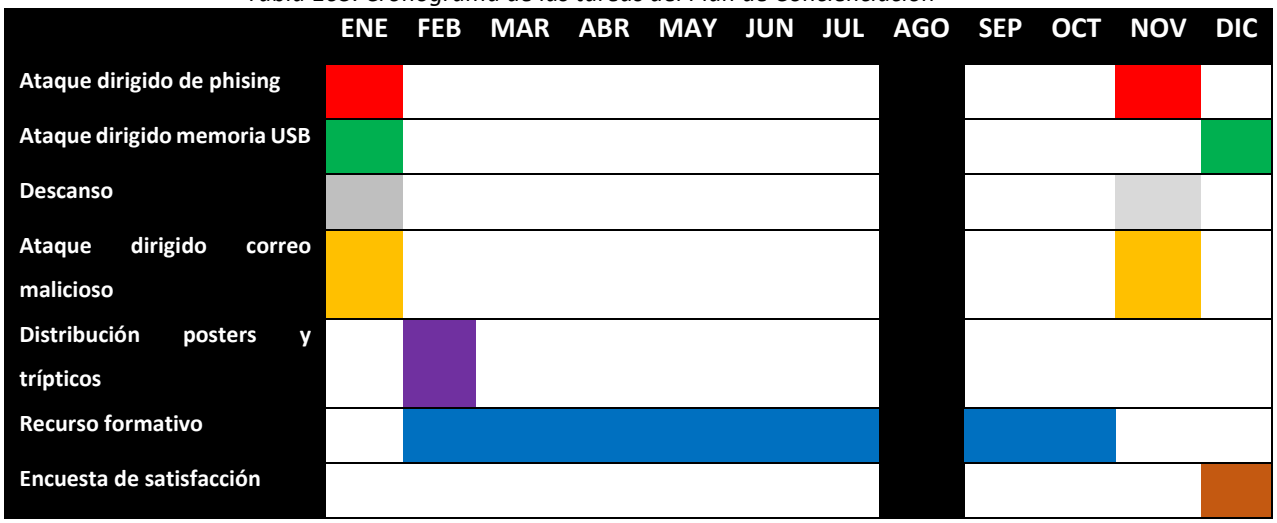
Basándonos en el Manual de Implantación de la campaña de formación y concienciación aportada por INCIBE [15], decidimos elaborar una propuesta de planificación de las tareas con sus tiempos de duración para esta. La planificación aportada por este manual es de 11 meses y medio de duración, por lo que necesitaremos establecerlo en 10 meses para que sea factible realizarlo a lo largo del año.

Tabla 164. Duración de las tareas del Plan de Concienciación

Tarea	Duración
Ataque dirigido de pishing	5 días laborables
Ataque dirigido memoria USB	5 días laborables
Descanso entre ataques	5 días laborables
Ataque enlace malicioso correo	5 días laborables
Distribución posters presentación y trípticos	1 día laborable
Recurso formativo	7 meses y 2 semanas
Ataque dirigido de pishing	5 días laborables
Ataque enlace malicioso correo	5 días laborables
Descanso entre ataques	5 días laborables
Ataque dirigido memoria USB	5 días laborables
Encuesta de satisfacción	1 día laborable

La siguiente imagen muestra un cronograma con el tiempo en semanas que ocupará la distribución de las tareas del plan:

Tabla 165. Cronograma de las tareas del Plan de Concienciación



10.1. Diseño de un ataque dirigido.

Para diseñar un ataque dirigido, lo primero que debemos evaluar es que vulnerabilidad deseamos explotar, el personal objetivo del ataque y los mecanismos o herramientas que se deben emplear para este.

Basándonos en el kit de INCIBE [15] diseñamos varios tipos de ciberataque inofensivos para comprobar el alcance que podría tener un ataque de verdad, para ello diseñaremos tres ataques diferentes que ejecutaremos.

10.1.1. Ataque de phishing con Gophish

Gopish es un framework de código abierto destinada a aprender a identificar y evitar el phishing en organizaciones y empresas.

El termino phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Para poner en marcha la campaña de phishing controlado en nuestra organización, para comprobar el estado de concienciación por parte de los empleados, tendremos que instalar la aplicación y configurarla de acuerdo al objetivo del ataque dirigido.

Antes de diseñar el ataque de Gophish, se ha analizado el tráfico de la red de los últimos meses para comprobar las webs más visitadas por los empleados, con esta información se han decidido los siguientes parámetros:

- **Web usada para phishing**: Amazon
- **Objetivo**: Empleados de oficina
- **Circunstancia**: Activación de servicio no deseado
- **Duración de la campaña**: 5 días laborales

El primer paso para configurar el ataque de phising es generar una cuenta de correo desde la que se enviarán los correos, por lo que es recomendado emplear una cuenta de correo genérica o emplear algún nombre que pueda llevar al engaño. Por ejemplo, para este caso, se podría crear una cuenta de correo que tuviese relación con Amazon (Fig.11).

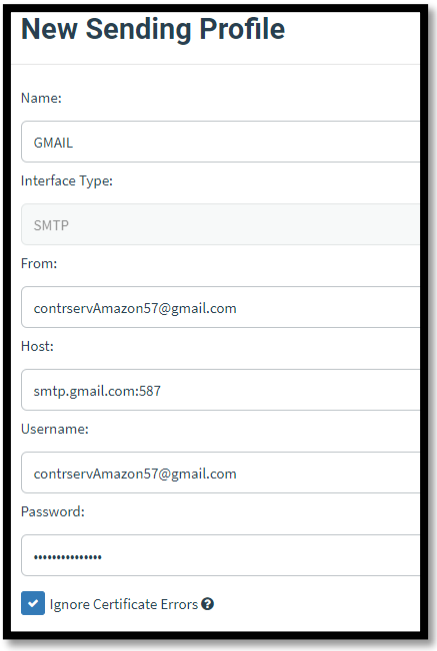


Figura 11. Configuración de la cuenta de correo para la campaña de phising en Gophish

Tras ello, empleando un correo de Amazon como base, se manipulara para hacer creer al usuario que se ha activado un servicio no deseado que va a comenzar a cobrarle cierta cantidad de dinero al mes (Fig.12), con el objetivo que pinche en los enlaces para entrar en la web y desactivarlo (Fig.13).

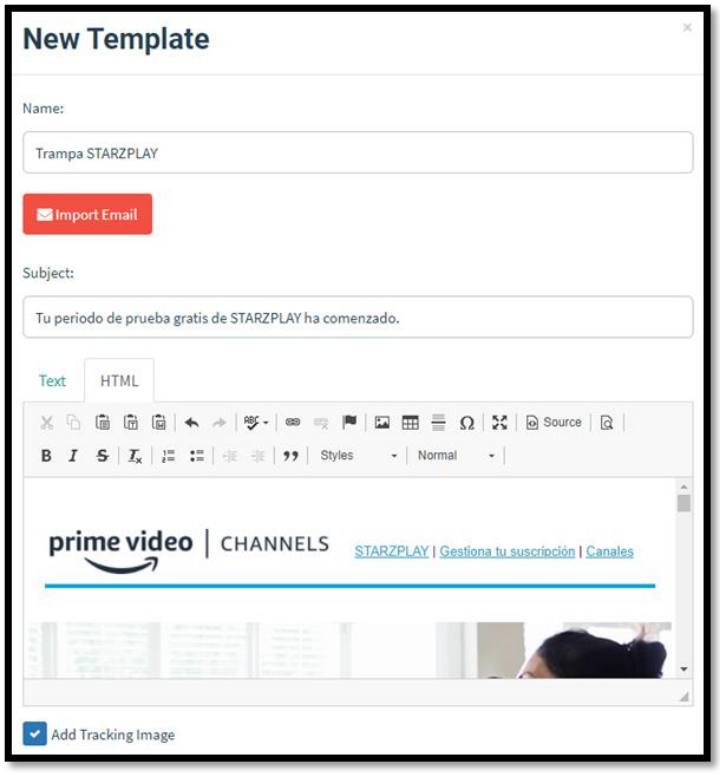


Figura 12. Configuración del correo de phishing para la campaña en Gophish

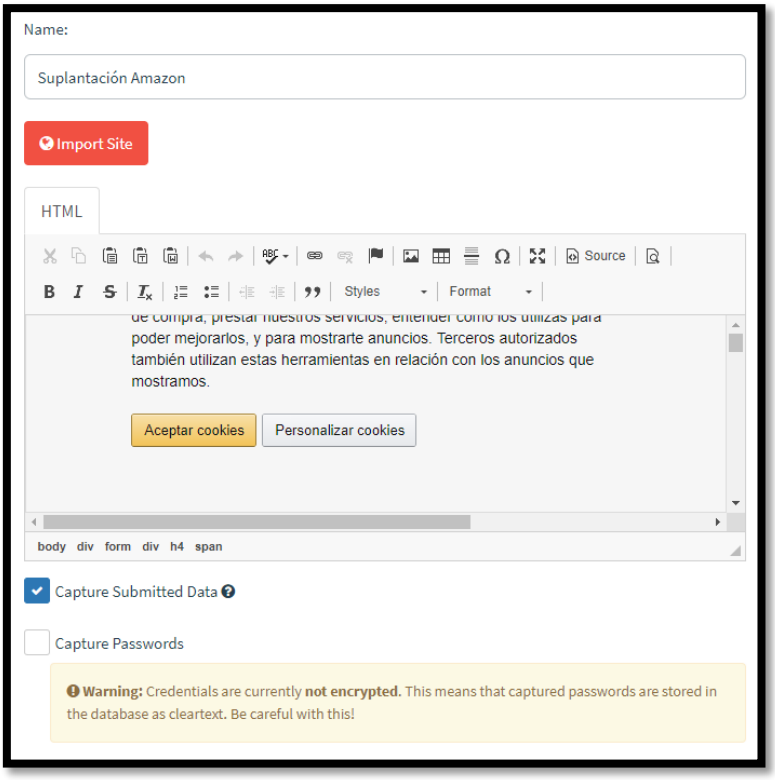


Figura 13. Configuración de la web donde se realizara el phishing con Gophish

A continuación, se configura el grupo de empleados al que irá dirigido el ataque de forma manual o empleando una libreta de direcciones y se lanza la campaña dirigida (Fig.15).

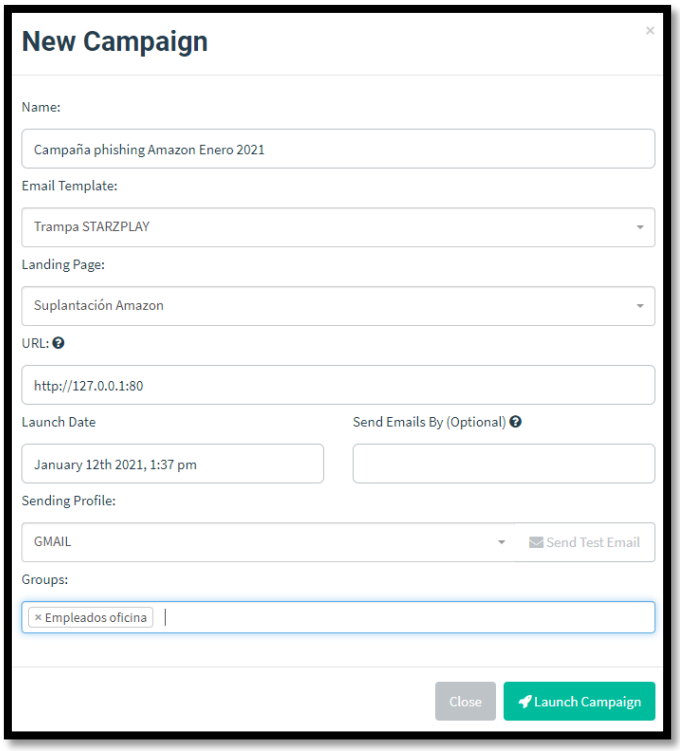


Figura 14. Configuración de la campaña de phishing en Gophish

Nota importante: Con Gophish existe la posibilidad de capturar las contraseñas de los usuarios (Fig.13) en el caso de que la página de phishing permita rellenar un formulario. Gophish no encripta las contraseñas obtenidas por lo que se podría vulnerar la privacidad de los usuarios y podría acarrear repercusiones legales, por lo que no se recomienda capturar contraseñas.

En el momento de activación de la campaña, se enviarán automáticamente correos (Fig.15) a los empleados configurados en el grupo. Y el servicio se mantendrá a la escucha de los eventos que la recepción que esos correos acarren (abrir el correo, entrar en la falsa web, pulsar en los enlaces o rellenar los formularios).

Figura 15. Correo de phishing recibido por los objetivos del ataque de Gophish de la campaña

En la interfaz web de Gophish (Fig.16) podremos comprobar el estado de la campaña en el momento de la consulta, así como el número de gente afectada, los datos introducidos y si el email ha sido denunciado como spam. Tras cinco días de actividad, la campaña se cerrará y se consultaran las estadísticas para comprobar el conocimiento de los empleados en materia de Phising.

Figura 16. Estadísticas de la campaña de phishing en Gophish

10.1.2. Ataque dirigido con memoria USB

El ataque dirigido con memoria USB consiste en preparar unos USB "extraviados" que contendrán ficheros trampa aunque muy tentadores para las víctimas (tales como información de nóminas o contrataciones/despidos), que al ser ejecutados registrará el éxito del ataque en un servicio que anotará desde donde se han conectado las memorias y en qué momento se han ejecutado los archivos trampa. En un caso real, estos archivos ejecutarían virus o ransomware.

Estos pendrives se dejarán "olvidados" en zonas comunes de la empresa, tales como la cafetería, en el suelo de la entrada, el baño o el parking.

Para diseñar el ataque dirigido con memoria USB, se han decidido los siguientes parámetros:

- **Almacenamiento**: Memorias USB de la empresa.
- **Objetivo**: Empleados de oficina y operarios.
- **Circunstancia**: Información nóminas y despidos.
- **Duración de la campaña**: 5 días laborales.

Los resultados de la campaña se comprobarán una vez finalizado el plazo de esta, recuperando los USB y guardándolos para la próxima vez.

10.1.3. Ataque dirigido con correo malicioso

El ataque dirigido con correo electrónico consiste en preparar un correo electrónico enviado desde una dirección ajena a la empresa, haciéndose pasar por servicio técnico o un cliente la empresa, que contendrán ficheros trampa que aparentan ser verídicos (tales como facturas, herramienta de seguridad…), que al ser ejecutados registrará el éxito del ataque en un servicio que anotará desde donde y en qué momento se han ejecutado los ficheros trampa. En un caso real, estos archivos ejecutarían virus o ransomware.

Para diseñar el ataque dirigido con correo electrónico, se han decidido los siguientes parámetros:

- **Medio**: Correo electrónico externo
- **Objetivo**: Empleados de oficina
- **Circunstancia**: Información facturas y servicio técnico
- **Duración de la campaña**: 5 días laborales

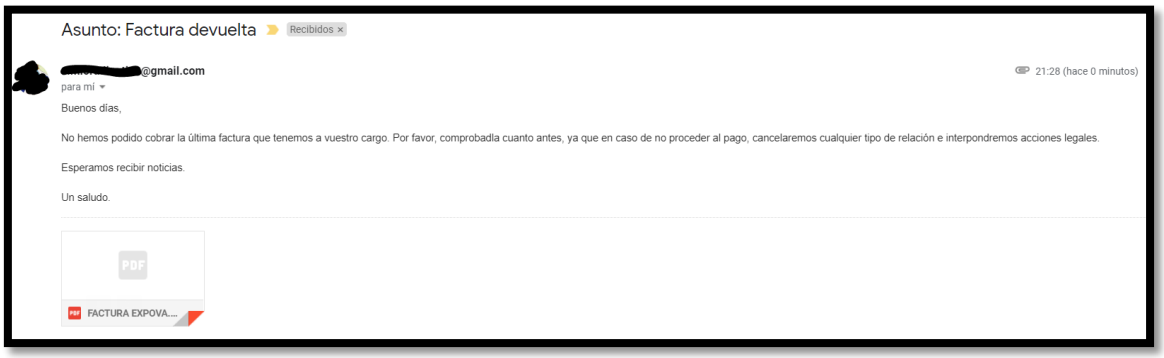


Figura 17. Correo con archivo malicioso en el ataque dirigido

Los resultados de la campaña se comprobarán una vez finalizado el plazo de esta.

10.2. Diseño de píldoras informativas.

Tras la ejecución de los ataques dirigidos y comprobar el alcance que han tenido en la empresa, se debe comenzar con la siguiente parte de la campaña, la distribución de posters presentación y trípticos, pequeños recursos con consejos de seguridad distribuidas de una forma no intrusiva y amigable, también conocidos como píldoras informativas.

Estos deberán ser impresos y colocados en lugares visibles donde el empleado los pueda leer tranquilamente (el ascensor, la sala de café, salas de reuniones, etc.).

Para el grupo empresarial Anónima S.L. se ha decidido diseñar un par de posters para ponerlos en la cafetería y en los tablones de anuncios del personal. Por lo que uno de ellos, irá dirigido a los empleados de oficina y el otro ya a todos los empleados incluyendo los operarios.

Figura 18. Carteles para la campaña de ciberseguridad

10.3. Recurso formativo.

A la vez que se comienza la distribución de las píldoras informativas, es necesario también comenzar con la distribución de los recursos informativos. En la hoja de ruta planteada para el grupo empresarial, se dispondrá de 7 meses y medio, para impartir algunos cursos de Ciberseguridad orientada según los departamentos o personal objetivo.

Cada uno de los recursos formativos se empleará para transmitir información útil sobre seguridad de la información y consejos o buenas prácticas a la hora de manejar información corporativa.

El objetivo es aportar los recursos formativos de una forma amigable y divertida para los empleados, para demostrarles la importancia de la ciberseguridad en la empresa.

Además, se podría incluir algunas charlas de personal de empresas afectadas por algún problema de ciberseguridad en su empresa para conocer de primera mano, lo que un problema así puede acarrear a los empleados y al conjunto empresarial.

Un ejemplo de planning para el recurso formativo, sería el siguiente:

Tabla 166. Planning propuesto para el recurso formativo

MES	SEMANA	FORMACIÓN
1	1	Seminario: La información. El activo imprescindible de tu organización.
	2	Actividades: La información. El activo imprescindible de tu organización.
	3	Descanso.
	4	Seminario: La información. Clasificación, cifrado y metadatos.
2	1	Actividades: La información. Clasificación, cifrado y metadatos.
	2	Descanso.
	3	Seminario: La información. Backups, borrado y tipos de almacenamiento.
	4	Actividades: La información. Backups, borrado y tipos de almacenamiento.
3	1	Descanso.
	2	Seminario: El correo electrónico. Principales fraudes y riesgos.
	3	Actividades: El correo electrónico. Principales fraudes y riesgos.
	4	Descanso.
4	1	Seminario: Contraseñas. Y medidas complementarias.
	2	Actividades: Contraseñas. Y medidas complementarias.
	3	Descanso.

	4	Seminario: El puesto de trabajo. Medidas de protección I.
5	1	Seminario: El puesto de trabajo. Medidas de protección I.
	2	Descanso.
	3	Seminario: El puesto de trabajo. Medidas de protección II.
	4	Seminario: El puesto de trabajo. Medidas de protección II.
6	1	Descanso.
	2	Seminario: Dispositivos móviles y teletrabajo. Riesgos y protección.
	3	Seminario: Dispositivos móviles y teletrabajo. Riesgos y protección.
	4	Descanso.
7	1	Seminario: Redes sociales. Medidas de seguridad para los perfiles de empresa.
	2	Seminario: Redes sociales. Medidas de seguridad para los perfiles de empresa.
	3	Descanso.
	4	Invitación de personas con experiencia en casos reales de cibercrimen.
8	1	Descanso.
	2	Mesa redonda.

10.4. Encuesta de satisfacción

Una vez finalizada la campaña de prevención y concienciación, la empresa enviará un pequeño cuestionario a los trabajadores de la empresa para preguntar que ha parecido la campaña y que aspectos deberían de mejorar o abordarse de otra forma en futuras campañas.

11. Conclusiones y trabajo futuro

El desarrollo del Plan Director de Seguridad de la Información de un grupo empresarial real, me ha permitido enfrentarme a todo un reto, ya que la gran cantidad de la activos de la información de los que depende el negocio me ha obligado a enfocar el proceso de análisis hacia una selección de aquellos activos más prioritarios para el negocio. Aunque no he realizado el estudio de forma íntegra, he seguido punto por punto los procedimientos para lograr realizar los análisis y evaluaciones que me han permitido finalmente generar los programas de seguridad, con los que el grupo empresarial podrá mejorar de forma significativa la seguridad de sus activos de la información. De este trabajo, he logrado extraer una serie de conclusiones que expondré a continuación.

La principal conclusión, que he logrado extraer, es la importancia de implantar un Sistema de Gestión de la Seguridad de la Información en la empresa, aunque sea con el simple objetivo de conocer los activos de la información de los que dispone la empresa y realizar el análisis de riesgos, para conocer a los peligros reales a los que se enfrenta la empresa en el día a día.

Otra conclusión extraída, es la necesidad de encontrar cuanto antes aquellos activos de la información más vitales para la organización, con el objetivo de poder centrar la atención de los planes de seguridad en reforzarlos y protegerlos. Al dar prioridad a estos activos, se puede justificar de una forma más sencilla la necesidad de realizar una inversión de recursos para el refuerzo de la seguridad en la organización.

También se ha reflejado la importancia de la creación de unas buenas políticas de seguridad de la información, algo de lo que paradójicamente la mayoría de las empresas suelen carecer, lo que supone una vulnerabilidad legal bastante importante, pues estas políticas son las que dictan lo que un empleado puede y no puede hacer con la información e infraestructura propiedad de la empresa.

Revisando los objetivos marcados al inicio del proyecto, se puede comprobar que se ha logrado cumplir la gran mayoría de los puntos propuestos. Se ha logrado cumplir la realización del análisis actual de la empresa, obteniendo aquellos activos que deben de ser protegidos con mayor premura; para a partir de este análisis lograr desarrollar un plan director de seguridad formado por una serie de proyectos considerados de especial importancia para proteger estos activos.

La implantación del Plan director de Seguridad aquí desarrollado quedaría pendiente como trabajo futuro inmediato por los responsables del grupo empresarial, quienes deberán de evaluar los planes aquí redactados y realizar la toma de decisiones necesaria acerca de que planes implantar, la prioridad de implantación de los proyectos y decidir el calendario de implantación.

Como trabajo a largo plazo quedaría la medición de los resultados obtenidos tras la implantación de los proyectos de seguridad para comprobar si se ha logrado una mejora en la seguridad de la información y el estudio del procedimiento y coste que supondría obtener la certificación ISO 27001 para el grupo empresarial.

Referencias

1. **INCIBE**. Ciberamenazas contra entornos empresariales: una guía de aproximación para el empresario. [en línea]. [consulta: 23 de Febrero de 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf
2. **INCIBE**. Decálogo ciberseguridad empresas: una guía de aproximación para el empresario. [en línea]. [consulta: 23 de Febrero de 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf
3. **Agencia Española de Protección de Datos**. Ley de Protección de Datos [en línea]. [consulta: 23 de Febrero de 2021]. Disponible en: https://www.agpd.es
4. **Ministerio de Asuntos Económicos y Transformación Digital**. Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico. [en línea]. [consulta: 23 de Febrero de 2021]. Disponible en: http://www.lssi.gob.es/paginas/Index.aspx
5. **Ministerio de Cultura y Deporte**. Ley de propiedad intelectual. [en línea]. [consulta: 23 de Febrero de 2021]. Disponible en: https://www.culturaydeporte.gob.es/cultura/propiedadintelectual/la-propiedad-intelectual/preguntas-mas-frecuentes/la-propiedad-intelectual.html
6. **International Chamber of Commerce**. ICC Cyber Security Guide for Business. [en línea]. [consulta: 23 de Febrero de 2021]. Disponible en: https://www.iccwbo.be/wp-content/uploads/2016/05/ICC-Cyber-security-guide-for-business.pdf
7. **ISO/IEC**. ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, New York: ISO/IEC, 2018. Disponible en: https://www.aenor.com/normas-y-libros/buscador-de-normas/iso?c=073906
8. **Agustín López Neira y Javier Ruiz Spohr**. Serie "27000". [en línea]. [consulta: 23 de Febrero de 2021]. Disponible en: https://www.iso27000.es/iso27000.html
9. **AMUTIO GÓMEZ, M. A., CANDAU, J. & MAÑAS, J. A. MAGERIT** – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. [en línea]. Madrid: Portal de Administración Electrónica, 2012. [Consulta: 15 de febrero 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

10. **AMUTIO GÓMEZ, M. A., CANDAU, J. & MAÑAS, J. A. MAGERIT** – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elemento. [en línea]. Madrid: Portal de Administración Electrónica, 2012. [Consulta: 15 de febrero 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf
11. **AMUTIO GÓMEZ, M. A., CANDAU, J. & MAÑAS, J. A. MAGERIT** – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de técnicas. [en línea]. Madrid: Portal de Administración Electrónica, 2012. [Consulta: 15 de febrero 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:130c633a-ee11-4e17-9cec-1082ceeac38c/2012_Magerit_v3_libro3_guia-de-tecnicas_es_NIPO_630-12-171-8.pdf
12. **Portal de la Administración Electrónica de España**. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [en línea]. [Consulta: 23 Febrero 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
13. **INCIBE**. Plan de contingencia y continuidad de negocio. [en línea]. [Consulta: 23 Febrero 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio
14. **INCIBE**. Plantilla ISO 27K. [en línea]. [Consulta: 9 Marzo 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad
15. **INCIBE**. Kit de concienciación. Manual de implantación [en línea]. [Consulta: 16 Febrero 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

Bibliografía

AMUTIO GÓMEZ, M. A., CANDAU, J. & MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método [en línea]. Madrid: Portal de Administración Electrónica, 2012. [Consulta: 15 de febrero 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XXu2nCgzbIV

AMUTIO GÓMEZ, M. A., CANDAU, J. & MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elemento [en línea]. Madrid: Portal de Administración Electrónica, 2012. [Consulta: 15 de febrero 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XXu2nCgzbIV

AMUTIO GÓMEZ, M. A., CANDAU, J. & MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas [en línea]. Madrid: Portal de Administración Electrónica, 2012. [Consulta: 15 de febrero 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XXu2nCgzbIV

ISO/IEC. ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, New York: ISO/IEC, 2018. Disponible en: https://www.aenor.com/normas-y-libros/buscador-de-normas/iso?c=073906

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. UNE-EN ISO/IEC 27000 Tecnología de la Información, Técnicas de seguridad, Sistemas de Gestión de Seguridad de la Información (SGSI), Visión de conjunto y vocabulario, Madrid: AENOR Internacional, 2019. Disponible en: https://www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0061478

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. UNE-EN ISO/IEC 27001 Tecnología de la Información, Técnicas de seguridad, Sistemas de Gestión de Seguridad de la Información (SGSI), Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015), Madrid: AENOR Internacional, 2017. Disponible en: https://www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0058428

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. UNE-EN ISO/IEC 27002 Tecnología de la Información, Técnicas de seguridad, Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015), Madrid: AENOR Internacional, 2017. Disponible en: https://www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0058429

INCIBE. Kit de concienciación. Manual de implantación [en línea]. [Consulta: 16 Febrero 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

INCIBE. Plan de contingencia y continuidad de negocio [en línea]. [Consulta: 23 Febrero 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

INCIBE. Ciberamenazas contra entornos empresariales: una guía de aproximación para el empresario [en línea]. [Consulta: 23 Febrero 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf

INCIBE. Decálogo ciberseguridad empresas: una guía de aproximación para el empresario [en línea]. [Consulta: 23 Febrero 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

INTERNATIONAL CHAMBER OF COMMERCE. ICC Cyber Security Guide for Business [en línea]. [Consulta: 23 Febrero 2021]. Disponible en: https://www.iccwbo.be/wp-content/uploads/2016/05/ICC-Cyber-security-guide-for-business.pdf

Anexo I – Estado Inicial. Controles de Seguridad de la Información en la organización según ISO/IEC 27001:2017

SECCIÓN A: REQUISITOS OBLIGATORIOS SGSI

Sección	Requerimientos ISO 27001	Estado
4	**Contexto de la organización**	
4,1	**Comprensión de la organización y de su contexto**	
4,1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Inicial
4,2	**Comprensión de las necesidades y expectativas de las partes interesadas**	
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Inicial
4.2 (b)	Determinar los requerimientos y obligaciones relevantes de seguridad de la información	Inicial
4,3	**Determinación del alcance del SGSI**	
4.3 (a)	La organización debe considerar las cuestiones externas e internas referidas en 4.1	Inicial
4.3 (b)	La organización debe considerar los requisitos referidos en 4.2	Inicial
4.3 (c)	La organización debe considerar las interfaces y dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones	Inicial
4,4	**SGSI**	
4,4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estándar	Inicial
5	**Liderazgo**	
5,1	**Liderazgo y compromiso**	
5,1 (a)	La administración debe demostrar liderazgo y compromiso por el SGSI asegurando que se establecen la política y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización	Inicial
5,1 (b)	La administración debe demostrar liderazgo y compromiso por el SGSI asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización	Inicial
5,1 (c)	La administración debe demostrar liderazgo y compromiso por el SGSI asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles	Inicial
5,1 (d)	La administración debe demostrar liderazgo y compromiso por el SGSI comunicando la importancia de una gestión de la seguridad	Inicial

	de la información eficaz y conforme con los requisitos del sistema de gestión de la seguridad de la información	
5,1 (e)	La administración debe demostrar liderazgo y compromiso por el SGSI asegurando que el sistema de gestión de la seguridad de la información consigue los resultados previstos	Inicial
5,1 (f)	La administración debe demostrar liderazgo y compromiso por el SGSI dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información	Inicial
5,1 (g)	La administración debe demostrar liderazgo y compromiso por el SGSI promoviendo la mejora continua	Inicial
5,1 (h)	La administración debe demostrar liderazgo y compromiso por el SGSI apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.	Inicial
5,2	**Política**	
5,2 (a)	La alta dirección debe establecer una política de seguridad de la información que sea adecuada al propósito de la organización	Inexistente
5,2 (b)	La alta dirección debe establecer una política de seguridad de la información que incluya objetivos de seguridad de la información (véase 6.2) o proporcione un marco de referencia para el establecimiento de los objetivos de seguridad de la información	Inexistente
5,2 (c)	La alta dirección debe establecer una política de seguridad de la información que incluya el compromiso de cumplir con los requisitos aplicables a la seguridad de la información	Inexistente
5,2 (d)	La alta dirección debe establecer una política de seguridad de la información que incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información.	Inexistente
5,2 (e)	La política de seguridad de la información debe estar disponible como información documentada	Inexistente
5,2 (f)	La política de seguridad de la información debe comunicarse dentro de la organización	Inexistente
5,2 (g)	La política de seguridad de la información debe estar disponible para las partes interesadas, según sea apropiado.	Inexistente
5,3	**Roles, responsabilidades y autoridades en la organización**	
5,3 (a)	La alta dirección debe asignar la responsabilidad y autoridad para asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de esta norma internacional	Repetible
5,3 (b)	La alta dirección debe asignar la responsabilidad y autoridad para informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información	Repetible
6	**Planificación**	
6,1	**Acciones para tratar los riesgos y oportunidades**	
6,1,1	**Consideraciones generales**	
6.1.1 (a)	Al planificar el SGSI, la organización debe considerar las cuestiones a las que se hace referencia en el apartado 4.1 y los requisitos incluidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario tratar con el fin de asegurar que el sistema de gestión de la seguridad de la información pueda conseguir sus resultados previstos	Inicial

6.1.1 (b)	Al planificar el SGSI, la organización debe considerar las cuestiones a las que se hace referencia en el apartado 4.1 y los requisitos incluidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario tratar con el fin de prevenir o reducir efectos indeseados	Inicial
6.1.1 (c)	Al planificar el SGSI, la organización debe considerar las cuestiones a las que se hace referencia en el apartado 4.1 y los requisitos incluidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario tratar con el fin de lograr la mejora continua.	Inicial
6.1.1 (d)	La organización debe planificar las acciones para tratar estos riesgos y oportunidades	Inicial
6.1.1 (e1)	La organización debe planificar la manera de integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información	Inicial
6.1.1 (e2)	La organización debe planificar la manera de evaluar la eficacia de estas acciones	Inicial
6,1,2	**Apreciación de riesgos de seguridad de la información**	
6.1.2 (a1)	Definir e implementar un proceso de análisis de riesgos de seguridad de la información que establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo los criterios de aceptación de los riesgos	Inexistente
6.1.2 (a2)	Definir e implementar un proceso de análisis de riesgos de seguridad de la información que establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información	Inexistente
6.1.2 (b)	Definir e implementar un proceso de análisis de riesgos de seguridad de la información que asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables	Inexistente
6.1.2 (c1)	Definir e implementar un proceso de análisis de riesgos de seguridad de la información que identifique los riesgos de seguridad de la información llevando a cabo el proceso de apreciación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información	Inexistente
6.1.2 (c2)	Definir e implementar un proceso de análisis de riesgos de seguridad de la información que identifique los riesgos de seguridad de la información identificando a los dueños de los riesgos	Inexistente
6.1.2 (d1)	Definir e implementar un proceso de análisis de riesgos de seguridad de la información que analice los riesgos de seguridad de la información valorando las posibles consecuencias que resultarían si los riesgos identificados en el punto 6.1.2 c) 1) llegasen a materializarse	Inexistente
6.1.2 (d2)	Definir e implementar un proceso de análisis de riesgos de seguridad de la información que analice los riesgos de seguridad de la información valorando de forma realista la probabilidad de ocurrencia de los riesgos identificados en el punto 6.1.2 c) 1)	Inexistente
6.1.2 (d3)	Definir e implementar un proceso de análisis de riesgos de seguridad de la información que analice los riesgos de seguridad de la información determinando los niveles de riesgo	Inexistente
6.1.2 (e1)	Definir e implementar un proceso de análisis de riesgos de seguridad de la información que evalúe los riesgos de seguridad de la información comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos en el punto 6.1.2 a)	Inexistente

6.1.2 (e2)	Definir e implementar un proceso de análisis de riesgos de seguridad de la información que evalúe los riesgos de seguridad de la información priorizando el tratamiento de los riesgos analizados	Inexistente
6,1,3	**Tratamiento de los riesgos de seguridad de la información**	
6.1.3 (a)	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información para seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos	Inexistente
6.1.3 (b)	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información para determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información	Inexistente
6.1.3 (c)	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información para comparar los controles determinados en el punto 6.1.3 b) con los del anexo A y comprobar que no se han omitido controles necesarios	Inexistente
6.1.3 (d)	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información para elaborar una “Declaración de Aplicabilidad”	Inexistente
6.1.3 (e)	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información para formular un plan de tratamiento de riesgos de seguridad de la información	Inexistente
6.1.3 (f)	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información para obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información por parte de los dueños de los riesgos	Inexistente
6,2	**Objetivos de seguridad de la información y planificación para su consecución**	
6,2 (a)	Los objetivos de seguridad de la información deben ser coherentes con la política de seguridad de la información	Inexistente
6,2 (b)	Los objetivos de seguridad de la información deben ser medibles	Inexistente
6,2 (c)	Los objetivos de seguridad de la información deben tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos	Inexistente
6,2 (d)	Los objetivos de seguridad de la información deben ser comunicados	Inexistente
6,2 (e)	Los objetivos de seguridad de la información deben ser actualizados, según sea apropiado	Inexistente
6,2 (f)	Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar lo que se va a hacer	Inexistente
6,2 (g)	Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar qué recursos se requerirán	Inexistente
6,2 (h)	Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar quién será responsable	Inexistente
6,2 (i)	Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar cuándo se finalizará	Inexistente

6,2 (j)	Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar cómo se evaluarán los resultados	Inexistente
7	**Soporte**	
7,1	**Recursos**	
7,1	Determinar y asignar los recursos necesarios para el SGSI	Inicial
7,2	**Competencia**	
7,2 (a)	La organización debe determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en seguridad de la información	Repetible
7,2 (b)	La organización debe asegurarse que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas	Repetible
7,2 (c)	La organización debe cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo	Inicial
7,2 (d)	La organización debe conservar la información documentada apropiada, como evidencia de la competencia	Repetible
7,3	**Concienciación**	
7,3 (a)	Las personas que trabajan bajo el control de la organización deben ser conscientes de la política de la seguridad de la información	Inexistente
7,3 (b)	Las personas que trabajan bajo el control de la organización deben ser conscientes de su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño en seguridad de la información	Inexistente
7,3 (c)	Las personas que trabajan bajo el control de la organización deben ser conscientes de las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información	Inexistente
7,4	**Comunicación**	
7,4 (a)	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI, incluyendo el contenido de la comunicación	Inexistente
7,4 (b)	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI, incluyendo cuando comunicar	Inexistente
7,4 (c)	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI, incluyendo a quién comunicar	Inexistente
7,4 (d)	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI, incluyendo quién debe comunicar	Inexistente
7,4 (e)	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI, incluyendo los procesos por los que debe efectuarse la comunicación	Inexistente
7,5	**Información documentada**	
7.5.1	**Consideraciones generales**	
7.5.1 (a)	El sistema de gestión de la seguridad de la información de la organización debe incluir la información documentada requerida por esta norma internacional	Inexistente
7.5.1 (b)	El sistema de gestión de la seguridad de la información de la organización debe incluir la información documentada que la	Inexistente

	organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información	
7.5.2	**Creación y actualización**	
7.5.2 (a)	Proveer la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia) a los documentos	Inicial
7.5.2 (b)	Proveer el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico) a los documentos	Inicial
7.5.2 (c)	Proveer una revisión y aprobación con respecto a la idoneidad y adecuación a los documentos	Inicial
7.5.3	**Control de la información documentada**	
7.5.3 (a)	La información documentada se debe controlar para asegurarse que esté disponible y preparada para su uso, dónde y cuándo se necesite	Inexistente
7.5.3 (b)	La información documentada se debe controlar para asegurarse que esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).	Inexistente
7.5.3 (c)	Para el control de la información documentada, la organización debe tratar la distribución, acceso, recuperación y uso	Inexistente
7.5.3 (d)	Para el control de la información documentada, la organización debe tratar el almacenamiento y preservación, incluida la preservación de la legibilidad	Inexistente
7.5.3 (e)	Para el control de la información documentada, la organización debe tratar el control de cambios	Inexistente
7.5.3 (f)	Para el control de la información documentada, la organización debe tratar la retención y disposición	Inexistente
8	**Operación**	
8,1	**Planificación y control operacional**	
8,1	Planificar, implementar, controlar y documentar el proceso de gestión de riesgos del SGSI (Tratamiento de riesgos)	Inexistente
8,2	**Apreciación de los riesgos de seguridad de la información**	
8,2	Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios	Inexistente
8,3	**Tratamiento de los riesgos de seguridad de la información**	
8,3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Inexistente
9	**Evaluación del desempeño**	
9,1	**Seguimiento, medición, análisis y evaluación**	
9,1 (a)	Se debe determinar a qué es necesario hacer seguimiento y qué es necesario medir, incluyendo procesos y controles de seguridad de la información	Inexistente
9,1 (b)	Se debe determinar los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos	Inexistente

9,1 (c)	Se debe determinar cuándo se deben llevar a cabo el seguimiento y la medición	Inexistente
9,1 (d)	Se debe determinar quién debe hacer el seguimiento y la medición	Inexistente
9,1 (e)	Se debe determinar cuándo se deben analizar y evaluar los resultados del seguimiento y la medición	Inexistente
9,1 (f)	Se debe determinar quién debe analizar y evaluar esos resultados	Inexistente
9,2	**Auditoría interna**	
9,2 (a1)	Planificar y realizar una auditoria interna del SGSI, para comprobar que el SGSI cumple con los requisitos propios de la organización	Inexistente
9,2 (a2)	Planificar y realizar una auditoria interna del SGSI, para comprobar que el SGSI cumple con los requisitos de esta norma internacional	Inexistente
9,2 (b)	Planificar y realizar una auditoria interna del SGSI, para comprobar que el SGSI está implementado y mantenido de manera eficaz	Inexistente
9,2 (c)	La organización debe planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas	Inexistente
9,2 (d)	La organización debe para cada auditoría, definir sus criterios y su alcance	Inexistente
9,2 (e)	La organización debe seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría	Inexistente
9,2 (f)	La organización debe asegurarse de que se informa a la dirección pertinente de los resultados de las auditorías	Inexistente
9,2 (g)	La organización debe conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.	Inexistente
9,3	**Revisión por la dirección**	
9,3 (a)	La revisión por la dirección debe incluir el estado de las acciones desde anteriores revisiones por la dirección	Inexistente
9,3 (b)	La revisión por la dirección debe incluir los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información	Inexistente
9,3 (c1)	La revisión por la dirección debe incluir la información sobre el comportamiento de la seguridad de la información, incluidas las tendencias relativas a no conformidades y acciones correctivas	Inexistente
9,3 (c2)	La revisión por la dirección debe incluir la información sobre el comportamiento de la seguridad de la información, incluidas las tendencias relativas a seguimiento y resultados de las mediciones	Inexistente
9,3 (c3)	La revisión por la dirección debe incluir la información sobre el comportamiento de la seguridad de la información, incluidas las tendencias relativas a resultados de auditoría	Inexistente
9,3 (c4)	La revisión por la dirección debe incluir la información sobre el comportamiento de la seguridad de la información, incluidas las tendencias relativas a el cumplimiento de los objetivos de seguridad de la información	Inexistente

9,3 (d)	La revisión por la dirección debe incluir los comentarios provenientes de las partes interesadas	Inexistente
9,3 (e)	La revisión por la dirección debe incluir los resultados de la apreciación de los riesgos y el estado del plan de tratamiento de riesgos	Inexistente
9,3 (f)	La revisión por la dirección debe incluir las oportunidades de mejora continua	Inexistente
10	**Mejora**	
10,1	**No conformidad y acciones correctivas**	
10,1	Cuando ocurra una no conformidad, la organización debe reaccionar ante la no conformidad, y según sea aplicable llevar a cabo acciones para controlarla y corregirla	Inexistente
10,1	Cuando ocurra una no conformidad, la organización debe reaccionar ante la no conformidad, y según sea aplicable hacer frente a las consecuencias	Inexistente
10,1	Cuando ocurra una no conformidad, la organización debe evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte, mediante la revisión de la no conformidad	Inexistente
10,1	Cuando ocurra una no conformidad, la organización debe evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte, mediante la determinación de las causas de la no conformidad	Inexistente
10,1	Cuando ocurra una no conformidad, la organización debe evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte, mediante la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir	Inexistente
10,1	Cuando ocurra una no conformidad, la organización debe implementar cualquier acción necesaria	Inexistente
10,1	Cuando ocurra una no conformidad, la organización debe revisar la eficacia de las acciones correctivas llevadas a cabo	Inexistente
10,1	Cuando ocurra una no conformidad, la organización debe si es necesario, hacer cambios al sistema de gestión de la seguridad de la información	Inexistente
10,1	La organización debe conservar información documentada, como evidencia de la naturaleza de las no conformidades y cualquier acción posterior llevada a cabo	Inexistente
10,1	La organización debe conservar información documentada, como evidencia de los resultados de cualquier acción correctiva	Inexistente
10,2	**Mejora continua**	
10,2	Mejora continua del SGSI	Inexistente

SECCIÓN B: ESTADO Y APLICABILIDAD DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

A5 Políticas de Seguridad de la información

A5.1 Directrices de gestión de la seguridad de la información

A5.1.1 Políticas para la seguridad de la información

- **¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada?** Existe una estructura jerarquizada de permisos pero no se encuentra formalmente documentada.
- **¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes?** No existen políticas de seguridad de la información como tal.
- **¿Cómo se autorizan, comunican, comprenden y aceptan las políticas?** Al no existir políticas de seguridad de la Información, todavía no existe un proceso formal de cómo comunicar y autorizar las políticas. Actualmente, para aceptar la Ley de Protección de datos, los empleados deben de firmar un documento en papel.
- **¿Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores?** Actualmente no, pero en el caso de disponer de una política de seguridad de la información, se obligaría a los empleados a aceptarla y firmarla.
- **¿Hay acuerdos adecuados de cumplimiento y refuerzo?** Al firmar un documento que contiene las cláusulas de seguridad, los empleados están comprometidos a cumplir, pero posteriormente no existe un seguimiento de cumplimiento.
- **¿Hay referencias cruzadas a buenas prácticas (como ISO27k, NIST SP800, CSC20 y otras normas y directrices relevantes)?** Actualmente no se disponen de referencias cruzadas a buenas prácticas.
- **¿Están las políticas bien escritas, legible, razonable y viable?** Al no existir políticas de seguridad de la Información, esta pregunta no puede ser respondida.
- **¿Incorporan controles adecuados y suficientes?** Al no existir políticas de seguridad de la Información, esta pregunta no puede ser respondida.
- **¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.?** Al no existir políticas de seguridad de la Información, esta pregunta no puede ser respondida.
- **¿Cuán madura es la organización en esta área?** Actualmente no se dispone de una política de seguridad de la información, pero se dispone de suficiente documentación para poder implementarla.

RESULTADO	COMENTARIO
INICIAL	No existe Política de Seguridad de la Información. Las políticas que existen no son gestionadas.

A5.1.2 Revisión de las políticas para la seguridad de la información

- **¿Todas las políticas tienen un formato y estilo consistentes?** Al no existir políticas de seguridad de la Información, esta pregunta no puede ser respondida.
- **¿Están todos al día, habiendo completado todas las revisiones debidas?** Al no existir políticas de seguridad de la Información, esta pregunta no puede ser respondida.
- **¿Se han vuelto a autorizar y se han distribuido?** Al no existir políticas de seguridad de la Información, esta pregunta no puede ser respondida.

RESULTADO	COMENTARIO
INEXISTENTE	No existe Política de Seguridad de la Información, por lo que no existe ninguna revisión.

A6 Organización de la seguridad de la información

A6.1 Organización interna

A6.1.1 Roles y responsabilidades en seguridad de la información

- **¿Se le da suficiente énfasis a la seguridad y al riesgo de la información?** No la suficiente, aunque se le da cierta importancia al sistema de roles de usuarios.
- **¿Hay apoyo de la administración?** Si.
- **¿Existe un foro de alta gerencia para analizar el riesgo de la información y las políticas, los riesgos y los problemas de seguridad?** No.
- **¿Los roles y las responsabilidades están claramente definidos y asignados a personas adecuadamente capacitadas?** Si.
- **¿Tiene cada rol responsabilidad específica con respecto al riesgo y la seguridad de la información?** Si, el sistema de grupos de usuarios y roles está definido para cada departamento.
- **¿Hay suficiente presupuesto para las actividades de seguridad y riesgo de la información?** Actualmente no, salvo casos aislados.

- **¿Hay coordinación dentro de la organización entre las unidades de negocio?** Si, la organización debe de estar coordinada para afrontar con éxito la actividad de negocio.
- **¿funciona efectivamente en la práctica?** Salvo algunos casos esporádicos, la organización se encuentra bien coordinada.
- **¿Existe una conciencia y un apoyo adecuados para la estructura de riesgo y seguridad de la información?** No, actualmente no existe una concienciación adecuada sobre la seguridad de la información.

RESULTADO	COMENTARIO
DEFINIDO	**Existe una separación por roles y se aplica según el esquema del organigrama de la empresa.**

A6.1.2 Segregación de tareas

- **¿Son los deberes / funciones segregados entre roles o individuos cuando sea relevante para reducir la posibilidad de incompetencia, negligencia y actividades inapropiadas?** Es muy relevante para mantener cualquier tipo de problema al mínimo e identificarlo antes de que se extienda en el proceso de negocio.
- **¿Se utiliza una matriz tipo RACI para mantener la identificación para cada tarea?** No, se utiliza otro tipo de identificación acordando un responsable y un periodo de actividad.
- **¿Existe una política que cubra la segregación de deberes?** No, no existe una política para ello.
- **¿Cómo llegan las decisiones con respecto a tal segregación?** Gerencia se encarga de reunir a los responsables de los departamentos para organizar la segregación.
- **¿Quién tiene la autoridad para tomar tales decisiones?** Gerencia y los responsables de departamentos.
- **¿Se realiza un seguimiento regular de las actividades y los registros de auditoría?** No, solo se realiza en caso de que haya algún problema.

RESULTADO	COMENTARIO
DEFINIDO	**Actualmente, las tareas son segregadas entre los diferentes roles de los departamentos. Aunque no están definidos formalmente.**

A6.1.3 Contacto con las autoridades

- **¿Hay disponible una lista de detalles de contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias?** Si, la empresa cuenta con una lista de contacto.
- **¿Quién es el responsable de contactar a las autoridades y en qué punto de un incidente / evento se realiza este contacto y cómo?** El departamento de recursos humanos.
- **¿La lista es actual y correcta?** Si, actualmente la lista es correcta.
- **¿Hay un proceso de mantenimiento?** Se actualiza todos los años o cada vez que hay un aviso por parte de las autoridades.

RESULTADO	COMENTARIO
ADMINISTRADO	Se dispone de listas de contacto revisadas por la dirección.

A6.1.4 Contacto con grupos de interés especial

- **¿Hay un contacto regular, con grupos especiales de interés, foros y listas de correo profesionales en riesgo de la información y la seguridad, tales como los capítulos locales de ISACA, ISC 2, ISSA, ISO27k?** No.
- **¿Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias, vulnerabilidades recientemente descubiertas y disponibilidad de parches?** No.

RESULTADO	COMENTARIO
INEXISTENTE	No existe contacto con grupos de interés especial.

A6.1.5 Seguridad de la información en la gestión de proyectos

- **¿Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos, incluidos todos los tipos de proyectos relacionados con la información, los nuevos desarrollos y los cambios / mejoras en los sistemas, aplicaciones y procesos existentes?** No, los riesgos de la información no son valorados en la gestión de proyectos.
- **¿La etapa del proyecto incluye actividades apropiadas?** No.

RESULTADO	COMENTARIO
INEXISTENTE	No se incluyen actividades de seguridad en los proyectos.

A6.2 Los dispositivos móviles y el teletrabajo

A6.2.1 Política de dispositivos móviles

- **¿Existen política y controles seguridad relacionados con los usuarios móviles?** No, aunque existen ciertas directrices de seguridad implantadas por el departamento de informática**.**
- **¿Se distinguen los dispositivos personales de los empresariales?** Si, se realiza la distinción.
- **¿Cómo se mantienen y controlan los sistemas portátiles para garantizar que estén actualizados sobre las definiciones de antivirus y los parches de seguridad?** El departamento de informática se encarga de realizar las actualizaciones.
- **¿Se emplean soluciones de MDM y soluciones MAM para controlar las aplicaciones, el acceso y el cifrado completo de disco?** No.

RESULTADO	COMENTARIO
REPETIBLE	Las configuraciones de los dispositivos móviles son aplicadas por el departamento de informática de manera informal.

A6.2.2 Teletrabajo

- **¿Los controles de seguridad para el teletrabajo son equivalentes a los de los lugares de trabajo de oficina?** Si, completamente. Los dispositivos usados para el teletrabajo son configurados de forma remota por el departamento de informática.
- **¿Existen disposiciones adecuadas para la autenticación del usuario (2FA), la seguridad de la red (Always-on-VPN), antivirus, copias de seguridad, parches, registro de seguridad y monitoreo, encriptación y continuidad del negocio?** Si, se utiliza siempre VPN siempre bien protegido con antivirus y se realiza monitorización de las conexiones por si se detecta alguna actividad fuera de lo normal.

RESULTADO	COMENTARIO
ADMINISTRADO	Las configuraciones de teletrabajo se encuentran documentadas y administradas por el departamento de informática.

A7 Seguridad relativa a los recursos humanos

A7.1 Antes del empleo

A7.1.1 Investigación de antecedentes

- **¿El proceso de evaluación previa al empleo toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo?** Si, las marca la empresa que colabora con la empresa en implantación de las medidas para cumplir con las nuevas leyes que se aplican año a año.
- **¿Se hace en la empresa o se subcontrata a un tercero?** Se hace en la propia empresa.
- **Si se subcontrata a un tercero, ¿Se han revisado sus procesos y se han considerado aceptables?** Si, cuando se contrata a un tercero se revisa la documentación de sus procesos.
- **¿Se hace contacto de referencias y una verificación de antecedentes, según corresponda durante el proceso de selección?** No, aunque para determinados puestos sí que se realiza el contacto de referencias para comprobar que son correctas.
- **¿Existen procesos de selección mejorados para los trabajadores en roles críticos?** Si, para esos casos se aplica un proceso más meticuloso.
- **¿Cómo se logra todo esto? ¿Hay un proceso documentado, consistente y repetible, que sea propiedad y mantenido por RRHH?** Si, tienen el proceso de selección de personal por promoción interna o externa.

RESULTADO	COMENTARIO
REPETIBLE	La investigación de antecedentes se realiza en determinados casos y dependiendo del rol al que serán asignados.

A7.1.2 Términos y condiciones del empleo

- **¿Están claramente definidos los términos y condiciones de empleo?** Sí, tienen un único convenio colectivo para las 4 empresas con sus diferentes funciones y tablas salariales.
- **¿Se hace distinción entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y los trabajadores en general?** Sí, pero de forma muy básica.
- **¿Se identifican responsabilidades específicas relacionadas con el riesgo y la seguridad de la información de acuerdo con la naturaleza de los roles?** No, se hace de forma muy básica.
- **¿Se mantienen registros para probar que los trabajadores entendieron, reconocieron y aceptaron sus obligaciones de seguridad de la información?** No.

RESULTADO	COMENTARIO
DEFINIDO	Los términos y condiciones se encuentran bien definidos, pero apenas se hace distinción entre los tipos de profesionales.

A7.2 Durante el empleo

A7.2.1 Responsabilidades de gestión

- **¿Existe un programa de concientización / educación sobre la seguridad de la información dirigido a la gerencia?** No.
- **¿Se hace de forma regular y está a día?** No.
- **¿El contenido y la naturaleza / formato / estilo de la información y las actividades de sensibilización son adecuados?** No existen.
- **¿Los gerentes reciben el conocimiento y la capacitación apropiados específicamente sobre su riesgo clave de información y roles y responsabilidades relacionados con la seguridad?** Son conscientes de ello.
- **¿Se provee información sobre la postura, estrategias y políticas de seguridad de la información de la organización?** No.

RESULTADO	COMENTARIO
INICIAL	No existe ningún programa de concienciación dirigido a la gerencia, pero ellos ya tienen claro su responsabilidad con la empresa.

A7.2.2 Concienciación, educación y capacitación en seguridad de la información

- **¿Están las competencias necesarias y los requisitos de capacitación / concienciación para los profesionales de seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente**? El personal del departamento de informática, está consciente en cuento a seguridad e intentan siempre mantenerse al día con nuevas actualizaciones y prepararse en cursos.
- **¿Existe un programa estructurado de sensibilización y capacitación sobre seguridad de la información para todos los tipos de trabajadores?** No, actualmente no existe tal programa.
- **¿Existe una estrategia o plan de comunicación, que incluya folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales y otros métodos?** No, aunque una vez al año se realiza un curso de prevención de riesgos laborales.

- **¿Se cubren los requisitos legales, reglamentarios, contractuales, políticos, responsabilidad personal, responsabilidades generales, puntos de contacto y otros recursos?** No.
- **¿Se actualiza el contenido para reflejar los riesgos de la información en evolución, como las amenazas emergentes, las vulnerabilidades recientemente identificadas y los incidentes, y los cambios, como las políticas nuevas / revisadas?** No.
- **¿Hay exámenes y ejercicios periódicos para verificar el nivel de conocimiento?** No.
- **¿Hay acciones de seguimiento para cualquiera que tenga problemas en dichas pruebas?** No.

RESULTADO	COMENTARIO
INICIAL	**Únicamente el departamento de informática esta concienciado de la importancia que requiere la seguridad de la información. Cada vez que descubren algún nuevo peligro, tratan de enviar correos para concienciar al personal.**

A7.2.3 Proceso disciplinario

- **¿Existe un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los trabajadores?** Nunca se ha dado un incidente de este tipo, pero en el caso de que ocurriese, seguramente sí que se abriría un expediente disciplinario.
- **¿Cómo se informa a los trabajadores sobre el proceso, incluidas las expectativas de la organización y sus derechos?** Al firmar el contrato laboral.
- **¿Está esto cubierto por contratos y acuerdos, capacitación inicial y conocimiento continuo?** No.
- **¿Se actualiza el proceso de forma regular?** No.

RESULTADO	COMENTARIO
INICIAL	**No existe proceso disciplinario dirigido a incidentes de seguridad de la información, por lo que se aplicarían los mismos que se emplearían a otro tipo de incidente en la empresa.**

A7.3 Finalización del empleo o cambio en el puesto de trabajo

A7.3.1 Responsabilidades ante la finalización o cambio

- **¿Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la seguridad de la información para los trabajadores que se mueven lateral o verticalmente dentro de la organización?** No, solamente se les avisa de sus nuevas responsabilidades y objetivos a cumplir.
- **¿Se tienen en cuenta las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias, despidos?** Si
- **¿Se tiene en cuenta la recuperación de los activos de información (documentos, datos, sistemas), las llaves, la eliminación de los derechos de acceso?** Si.

RESULTADO	COMENTARIO
REPETIBLE	**Existen procedimientos establecidos por recursos humanos, pero los departamentos requieren de una mayor comunicación para agilizar el proceso.**

A8	**Gestión de activos**
A8.1	**Responsabilidad sobre los activos**
A8.1.1	**Inventario de activos**

- **¿Hay un inventario de activos de la información?** Si, contiene información sobre el hardware y software del que se dispone en la empresa.
- **¿Contiene la siguiente información?**
  - **Datos digitales** No
  - **Información impresa** No
  - **Software** Si
  - **Infraestructura** Si
  - **Servicios de información y proveedores de servicios** Si
  - **Seguridad física** No
  - **Relaciones comerciales** No
  - **Las personas** Si
- **¿A quién pertenece el inventario?** Al departamento de informática

- **¿Cómo se mantiene el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI?** Se intenta mantener siempre actualizado, cada vez que se adquiere un nuevo activo, se cambia de lugar/propietario o se da de baja.
- **¿Es suficientemente detallado y está estructurado adecuadamente?** Está bien detallado y estructurado, pero se podría mejorar incluyendo información más exacta sobre su uso y responsables.

RESULTADO	COMENTARIO
DEFINIDO	**El departamento cuenta con un inventario de activos bien definido, aunque carece de información acerca de los activos de la información.**

A8.1.2 Propiedad de los activos

- **¿Los activos tienen propietario de riesgo?** Los equipos de riesgo como servidores o dispositivos de red, están bajo la responsabilidad del departamento de informática.
- **¿Los activos tienen responsable técnico?** Si, el departamento de informática se hace cargo de las incidencias software y hardware que puedan ocurrir dentro de la organización.
- **¿Cómo se asigna la propiedad poco después de crear o adquirir los activos críticos?** Los activos críticos nada más adquirirlos se asigna la responsabilidad al personal del departamento de informática.
- **¿Cómo se etiquetan los activos?** Si se tratan de activos hardware, se les añade una etiqueta QR, para que el departamento de informática pueda identificarlos. Además, se incorporan al inventario de la organización.
- **¿Cómo se informa ante incidentes de seguridad de la información que los afectan?** Ante un incidente de seguridad, se avisa al responsable del departamento de informática por teléfono.

RESULTADO	COMENTARIO
REPETIBLE	**La responsabilidad de los activos de la información recae toda sobre el departamento de informática. No se considera la responsabilidad de los empleados.**

A8.1.3 Uso aceptable de activos

- **¿Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.?** No.
- **¿Cubre el comportamiento del usuario en Internet y en las redes sociales?** No.
- **¿Se permite el uso personal de los activos de la empresa?** Sí, pero solo para casos puntuales.
- **En caso afirmativo, ¿En qué medida y cómo se controla / asegura esto?** No se controla, cae en la responsabilidad del empleado.
- **¿Se describe de forma explícita lo qué constituye un uso inapropiado?** No.
- **¿Se distribuye esta información a toda la empresa?** No.
- **¿El uso de la criptografía cumple con todas las leyes, acuerdos / contratos y normativas relevantes?** Si.

RESULTADO	COMENTARIO
REPETIBLE	**No existe una política sobre el uso aceptable de los recursos tecnológicos, pero en el caso de que se presente algún incidente, se avisa al empleado de sus responsabilidades y del uso profesional de los activos.**

A8.1.4 Devolución de activos

- **¿Existe un procedimiento para recuperar los activos tras una baja o despido?** Sí, pero no existe documentación al respecto.
- **¿Es un procedimiento automatizado o manual?** Es un procedimiento manual.
- **Si es manual, ¿Cómo se garantiza que no haya desvíos?** Se trata con el empleado, informándole que debe entregar el dispositivo a ser retirado.

RESULTADO	COMENTARIO
DEFINIDO	**El departamento de informática es informado de las bajas para pedir al empleado la devolución del equipo.**

A8.2 Clasificación de la información

A8.2.1 Clasificación de la información

- **¿Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información?** Se realiza una clasificación muy básica y es responsabilidad de cada departamento.
- **¿La clasificación es impulsada por obligaciones legales o contractuales?** Legales.
- **¿La clasificación se basa en los requisitos de confidencialidad, integridad y disponibilidad?** No.
- **¿Se utilizan marcas apropiadas en los activos en función de la clasificación de la información que contienen?** Si.
- **¿El personal conoce los requisitos de seguridad correspondientes para el manejo de materiales clasificados?** No.

RESULTADO	COMENTARIO
INICIAL	Solo los responsables de la información son conscientes de si la información debe ser clasificada y protegida.

A8.2.2 Etiquetado de la información

- **¿Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica?** Si, aunque solo para los activos más críticos.
- **¿Está sincronizado con la política de clasificación de la información?** No.
- **¿Cómo se garantiza el correcto etiquetado?** No se garantiza.
- **¿Cómo se garantiza que solo aquellos con permisos de acceso aprobados accedan a la información de la clasificación relevante?** Solo el departamento de informática tiene acceso a esa información.
- **¿Cómo se garantiza que no haya acceso no autorizado?** Usuario y contraseña.
- **¿Se revisan los niveles de clasificación en intervalos predefinidos?** No.

RESULTADO	COMENTARIO
INICIAL	El etiquetado es muy básico y no garantiza su seguridad.

A8.2.3 Manipulación de la información

Más allá de A.8.2.1

- **¿Están los niveles de clasificación adecuadamente asignados a los activos?** No
- **¿Se considera los siguiente?** -

  Método de etiquetado, transferencia, almacenamiento, manejo de medios extraíbles, eliminación de medios electrónicos y físicos, divulgación, intercambio, intercambio con terceros, etc. -

RESULTADO	COMENTARIO
INEXISTENTE	No existe procedimiento para el manipulado de la información.

A8.3 Manipulación de los soportes

A8.3.1 Gestión de soportes extraíbles

- **¿Existe un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles?** No.
- **¿Los medios extraíbles están debidamente etiquetados y clasificados?** Si, poseen una etiqueta indicando que son propiedad de la empresa.
- **¿Los medios se mantienen y almacenan de forma adecuada?** No.
- **¿Hay controles apropiados para mantener la confidencialidad de los datos almacenados?** No.

RESULTADO	COMENTARIO
INICIAL	La responsabilidad de los soportes extraíbles recae sobre su propietario final.

A8.3.2 Eliminación de soportes

Más allá de A.8.3.1

- **¿Existen una política específica y documentación de obligaciones contractuales, legales o reglamentarias para la eliminación de los medios?** Sí, pero no como documento escrito.
- **¿Se documenta la aprobación en cada etapa para la eliminación de los medios?** No, son eliminados directamente por el personal del departamento de informática.

- **¿Los datos que aún deben conservarse se copian en otros medios y se verifican antes de su eliminación?** Si.
- **¿Se tiene en cuenta los periodos de retención?** Si.
- **¿Los datos particularmente confidenciales se eliminan de forma segura (borrado criptográfico, desmagnetización o destrucción física)?** No, nunca se ha dado el caso.

RESULTADO	COMENTARIO
DEFINIDO	Existen procesos establecidos para la eliminación de los medios extraíbles.

A8.3.3 Soportes físicos en tránsito

- **¿Se utiliza un transporte o servicio de mensajería confiable?** Si
- **¿Se utiliza un mecanismo de cifrado adecuado durante el proceso de transferencia?** Si, se encripta.
- **¿Se verifica la recepción por el destino?** Si.

RESULTADO	COMENTARIO
ADMINISTRADO	El envío de soportes físicos es gestionado por el departamento de informática y servicio de mensajería de la empresa.

A9 Control de acceso

A9.1 Requisitos de negocio para el control de acceso

A9.1.1 Política de control de acceso

- **¿Existe una política de control de acceso?** Si, para acceder a los sistemas todos los usuarios deben emplear su usuario y contraseña.
- **¿Es consistente con la política de clasificación?** Si, depende del rol de usuario.
- **¿Hay una segregación de deberes apropiada?** Si, de acuerdo al departamento.
- **¿Existe un proceso documentado de aprobación de acceso?** No.
- **¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?** Gerencia, recursos humanos y el departamento de informática.

RESULTADO	COMENTARIO
DEFINIDO	El control de acceso es simple pero cumple con su función, dar

	acceso a las aplicaciones y datos de acuerdo con su puesto de trabajo y necesidades

A9.1.2 Acceso a las redes y a los servicios de red

- **¿Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado?** Si, solo pueden emplearlo los usuarios a los que el departamento de informática les da permiso bajo orden de gerencia.
- **¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados?** No.
- **¿Cómo monitoriza la red para detectar acceso no autorizado?** Mediante la comprobación de los LOGs y avisos por correo de los dispositivos al ver actividad sospechosa.
- **¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)?** No.
- **¿La organización mide la identificación y los tiempos de respuesta ante incidentes?** No.

RESULTADO	COMENTARIO
DEFINIDO	**El acceso a la red se encuentra bien definido por el departamento informático, aunque no cuenta con un procedimiento documentado.**

A9.2 Gestión de acceso de usuario

A9.2.1 Registro y baja de usuario

- **¿Se utiliza un ID de usuario únicos para cada usuario?** Cada usuario cuenta con su propio nombre de usuario para acceder a los sistemas.
- **¿Se genera en función a una solicitud con aprobaciones y registros apropiados?** El departamento de informática genera el usuario cuando recursos humanos se lo solicita.
- **¿Se deshabilitan los ID de usuario de forma inmediata tas una baja o despido?** Si, se desactivan de inmediato.
- **¿Existen una comunicación eficiente ente la Administración de Seguridad y Recursos Humanos?** Si.
- **¿Existe una revisión / auditoría periódica para identificar y deshabilitar los ID de usuario redundantes?** Si, una vez al año se revisa.

- **¿Se eliminan los ID deshabilitados después de confirmar que ya no son necesarios?** No se suelen eliminar por si acaso.
- **¿Qué impide que los ID de usuario sean reasignados a otros usuarios?** Que el registro de acciones se debe conservar para el usuario original.

RESULTADO	COMENTARIO
ADMINISTRADO	El registro de los usuarios se realiza desde el dominio para conservarlo para todos los sistemas.

A9.2.2 Provisión de acceso de usuario

- **¿El acceso a sistemas y servicios de información se basa en las necesidades del negocio?** Si, depende del rol del usuario y de su departamento.
- **¿Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones?** Si.
- **¿Existe un registro documental de la solicitud y aprobación de acceso?** No.

RESULTADO	COMENTARIO
REPETIBLE	Cada usuario se encuentra en un grupo de usuarios. Los grupos de usuarios se establecen según las necesidades de acceso de cada grupo.

A9.2.3 Gestión de privilegios de acceso

Más allá de A.9.2.2

- **¿Hay un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios?** Si, una vez al año se realiza el proceso de evaluación de usuarios para comprobar que nadie cuenta con más privilegios de los que le corresponden.
- **¿Se genera un ID de usuario separado para otorgar privilegios elevados?** No.
- **¿Se ha establecido una caducidad para los ID de usuario con privilegios?** No.
- **¿Se controlan las actividades de los usuarios privilegiados de forma más detallada?** Si.

RESULTADO	COMENTARIO
INICIAL	Se realiza una gestión muy básica y suficiente de los privilegios de acceso.

A9.2.4 Gestión de la información secreta de autenticación de los usuarios

- **¿Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.?** No, todos los empleados comparten la misma contraseña de acceso.
- **¿Se verifica rutinariamente si hay contraseñas débiles?** No.
- **¿Se requiere confirmar la identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas?** No.
- **¿Se transmite dicha información por medios seguros?** No.
- **¿Se generan contraseñas temporales suficientemente fuertes?** No.
- **¿Se cambian las contraseñas por defecto de los fabricantes?** Si, las modifican y almacenan los responsables del departamento de informática.
- **¿Se recomienda a los usuarios usar el software adecuado de protección de contraseñas?** No.
- **¿Se almacenen de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones?** Si.

RESULTADO	COMENTARIO
INICIAL	Aunque todos los usuarios comparten la misma contraseña, en gerencia cada usuario tiene su contraseña individual. El departamento de informática gestiona y almacena las claves encriptadas de todos los dispositivos de la empresa.

A9.2.5 Revisión de los derechos de acceso de usuario

- **¿Se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones?** No.
- **¿Participan en dicha revisión los "propietarios" para verificar cambios en las funciones de los usuarios?** No.
- **¿Se revisan los derechos de acceso para usuarios con privilegios de forma más exhaustiva y frecuente?** No.

RESULTADO	COMENTARIO
INEXISTENTE	No se realiza ninguna revisión de los derechos de acceso de los usuarios.

A9.2.6 Retirada o reasignación de los derechos de acceso

- **¿Existe un proceso de ajuste de derechos de acceso?** Si.
- **¿Tiene en cuenta empleados, proveedores y contratistas al finalizar o cambiar su empleo, contrato o acuerdo?** Si, recursos humanos o dirección avisa de ello al departamento de informática.
- **¿Incluye el acceso físico a las instalaciones y el acceso lógico a la red?** Si.
- **En casos en los que se usan credenciales compartidas, ¿Se cambian las contraseñas cuando ocurren ceses o despidos de empleados que las usan?** No.

RESULTADO	COMENTARIO
DEFINIDO	La retirada de los derechos de acceso se realiza deshabilitando el usuario del dominio.

A9.3 Responsabilidades del usuario

A9.3.1 Uso de la información secreta de autenticación

- **¿Cómo se asegura la confidencialidad de las credenciales de autenticación?** No se asegura.
- **¿Existe un proceso de cambio de contraseñas en caso de ser comprometida?** En caso de ser comprometida, se debe avisar el departamento de informática. Al usarse la misma contraseña para la mayor parte de usuarios, se cambiaría la contraseña a todo el personal de la empresa.
- **¿Existen controles de seguridad relativas a las cuentas compartidas?** No.

RESULTADO	COMENTARIO
INEXISTENTE	No es posible asegurar la confidencialidad de las contraseñas

A9.4 Control de acceso a sistemas y aplicaciones

A9.4.1 Restricción del acceso a la información

Más allá de A.9.2.2

- **¿Existen controles de acceso adecuados?** De usuario y contraseña, registro logs de intentos de inicio de sesión.
- **¿Se identifican los usuarios de forma individual?** Si

- **¿Cómo se definen, autorizan, asignan, revisan, gestionan y retiran los derechos de acceso, los permisos y las reglas asociadas?** Se gestiona el acceso de a los recursos dependiendo de su departamento y su puesto de trabajo. Si se requiere que se otorguen o retiren permisos, se comunica al departamento de informática para que realice el cambio oportuno.

RESULTADO	COMENTARIO
REPETIBLE	El control solo se puede realizar mediante la monitorización de logs y no existe registro de cambio de permisos.

A9.4.2 Procedimientos seguros de inicio de sesión

- **¿Se muestra una pantalla de advertencia en el proceso de inicio de sesión para disuadir el acceso no autorizado?** Solo en el caso de conexiones desde fuera de la red de la empresa (tal como VPN).
- **¿Cómo se autentican las identidades de usuario durante el proceso de inicio de sesión?** Usuario y contraseña, que se comprueba en el servidor de dominio de la empresa.
- **¿Se utiliza autenticación multifactor para sistemas / servicios / conexiones remotas críticas a través de VPN s etc.?** No se usa.
- **¿La información de inicio de sesión solo se valida una vez imputadas las credenciales?** Si.
- **¿Las contraseñas no válidas desencadenan demoras o bloqueos, entradas de registro y alertas / alarmas?** Se generan avisos en logs y tras varios intentos fallidos desencadena una demora.
- **¿Se registran los inicios de sesión exitosos?** Si, en los logs.
- **¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?** Un empleado del departamento de informática comunica en persona las contraseñas.

RESULTADO	COMENTARIO
REPETIBLE	Existe un procedimiento, pero no se encuentra formalizado.

A9.4.3 Sistema de gestión de contraseñas

- **¿Los sistemas requieran una fortaleza de contraseñas establecidos en las políticas y estándares corporativos?** No.
- **¿Las reglas tienen en cuenta lo siguiente?** No. Únicamente la de administración.

- **Longitud mínima de la contraseña**
- **Evitan la reutilización de un número específico de contraseñas**
- **Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.)**
- **Requiere el cambio forzado de contraseñas en el primer inicio de sesión**
- **Esconde la contraseña durante la imputación**

- **¿Se almacenan y transmiten de forma segura (cifrado)?** No se transmiten. Es un empleado del departamento de informática el que se la comunica al empleado.

RESULTADO	COMENTARIO
INICIAL	**Unicamente las contraseñas empleadas por gerencia y el departamento de informática, cuentan con cierta fortaleza.**

A9.4.4 Uso de utilidades con privilegios del sistema

- **¿Quién controla los servicios privilegiados?** Los empleados del departamento TIC.
- **¿Quién puede acceder a ellos, bajo qué condiciones y con qué fines?** Los empleados del departamento TIC y los responsables de Gerencia en caso de necesidad.
- **¿Se verifica que estas personas necesidad comercial para otorgar el acceso según su roles y responsabilidades?** En el caso de que alguien necesite acceder, debe pedir permiso al departamento de informática, quienes se pondrán en contacto con gerencia para evaluar la petición.
- **¿Existe un proceso auditable de aprobación, y cada instancia de su uso está registrado?** No.
- **¿Se tiene en cuenta la segregación de tareas?** Si.

RESULTADO	COMENTARIO
DEFINIDO	**El departamento de informática al administrar el acceso a las utilidades con privilegios, es el que realizara todas aquellas acciones que requieran de privilegios de sistema.**

A9.4.5 Control de acceso al código fuente de los programas

- **¿El código fuente se almacena en una o más bibliotecas de programas fuente o repositorios?** Se emplean repositorios locales y externos.

- **¿El entorno es seguro, con un acceso adecuado, control de versiones, monitoreo, registro, etc.?** Es seguro, si se modifica algo queda constancia.
- **¿Cómo se modifica el código fuente?** Se modifica, se prueba y finalmente pasa al entorno de producción.
- **¿Cómo se publica y se compila el código?** El departamento de informática es quien compila y publica el código una vez que se comprueba su buen funcionamiento.
- **¿Se almacenan y revisan los registros de acceso y cambios?** Si, queda constancia de todos los cambios.

RESULTADO	COMENTARIO
DEFINIDO	Todo código fuente se encuentra almacenado de forma correcta y segura. A este solo tiene acceso el departamento de informática.

A10 Criptografía

A10.1 Controles criptográficos

A10.1.1 Política de uso de los controles criptográficos

- **¿Existe una política que cubra el uso de controles criptográficos?** No.
- **¿Cubre lo siguiente?** -
    - **Los casos en los que información debe ser protegida a través de la criptografía**
    - **Normas que deben aplicarse para la aplicación efectiva**
    - **Un proceso basado en el riesgo para determinar y especificar la protección requerida**
    - **Uso de cifrado para información almacenada o transferida**
    - **Los efectos de cifrado en la inspección de contenidos de software**
    - **Cumplimiento de las leyes y normativas aplicables**
- **¿Se cumple con la política y requerimientos de cifrado?** No, solo se cifran las copias de seguridad.

RESULTADO	COMENTARIO
INICIAL	No existe una política de criptografía como tal, pero el departamento de informática es consciente de que algunos activos sensibles deben ser cifrados.

A10.1.2 Gestión de claves

- **¿La política de criptografía abarca todo el ciclo de vida de la gestión de claves (de principio a fin)?** No.
- **¿Se protege el equipo utilizado para generar, almacenar y archivar claves criptográficas?** Si.
- **¿Se generan claves diferentes para sistemas y aplicaciones?** Si.
- **¿Se evitan claves débiles?** Si.
- **¿Existen reglas sobre cambio / actualización de claves (ej. autorizar, emitir, comunicar e instalar claves)?** No.
- **¿Se hacen copias de respaldo de las claves?** No.
- **¿Se registran las actividades clave de gestión?** No.
- **¿Cómo se cumplen todos estos requisitos?** –

RESULTADO	COMENTARIO
INICIAL	El departamento de informática cuenta con algunas claves criptográficas que se emplean para cifrar la información según la importancia que tenga.

A11 Seguridad física y del entorno

A11.1 Áreas seguras

A11.1.1 Perímetro de seguridad física

- **¿Las instalaciones se encuentran en una zona de riesgo?** No, se encuentran en un polígono industrial en el que no suele haber incidentes.
- **¿Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.)?** Si, están definidos.
- **¿El techo exterior, las paredes y el suelo son de construcción sólida?** Si.
- **¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado?** Si.
- **¿Las puertas y ventanas son fuertes y con cerradura?** Si.
- **¿Se monitorea los puntos de acceso con cámaras?** Si.

- **¿Existe un sistema de detección de intrusos y se prueba periódicamente?** Si, se hacen simulacros cada mes.

RESULTADO	COMENTARIO
OPTIMIZADO	El grupo empresarial da mucha importancia a la seguridad exterior de sus instalaciones.

A11.1.2 Controles físicos de entrada

- **¿Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)?** La empresa cuenta con cerraduras de seguridad, cámaras de vigilancia y sensores de movimiento.
- **¿Hay procedimientos que cubran las siguientes áreas?** -
    - **Cambio regular código de acceso** No.
    - **Inspecciones de las guardias de seguridad** Si.
    - **Visitantes siempre acompañados y registrados en el libro de visitantes** No.
    - **Registro de movimiento de material** Si.
    - **Entrada a áreas definidas del edificio según roles y responsabilidades (acceso a CPD, salas de comunicación y otras áreas críticas)** No.
- **¿Se utiliza autenticación multi-factor de autenticación (ej. Biométrico más el código PIN)?** No.
- **¿Se requiere para las áreas críticas?** No.
- **¿Existe un registro de todas las entradas y salidas?** No.

RESULTADO	COMENTARIO
DEFINIDO	La empresa cuenta una seguridad suficiente para proteger sus activos.

A11.1.3 Seguridad de oficinas, despachos y recursos

- **¿Están los accesos (entrada y salida) de las instalaciones físicamente controlas (ej. Detectores de proximidad, CCTV)?** Si, están vigiladas por cámaras de seguridad y sensores de proximidad/movimiento.
- **¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos?** Durante la jornada de trabajo

pueden llegar a ser insuficientes, mientras que cuando la empresa está cerrada, la seguridad es muy buena.

- **¿Se tiene en cuenta los activos de información almacenados, procesados o utilizados en dichas ubicaciones?** No demasiado.

RESULTADO	COMENTARIO
REPETIBLE	**La empresa cuenta con buenas medidas de seguridad en las entradas de las instalaciones, pero no dispone de recepción, por lo que puede entrar cualquiera usando ingeniería social.**

A11.1.4 Protección contra las amenazas externas y ambientales

- **¿Qué tipo de protecciones existen contra el fuego, el humo, inundaciones, rayos, intrusos, vándalos, etc.?** Existe protección contra incendios, intrusos, fallos eléctricos…
- **¿Existe un procedimiento de recuperación de desastres?** Si.
- **¿Se contemplan sitios remotos?** Si, en caso de necesidad se puede desplazar a la gente de nave.

RESULTADO	COMENTARIO
DEFINIDO	**La empresa cuenta con medidas de seguridad suficientes para proteger la empresa de amenazas externas o ambientales.**

A11.1.5 El trabajo en áreas seguras

- **¿Se verifican al final del día las oficinas, las salas de informática y otros lugares de trabajo?** No.
- **¿Se hace un análisis para evaluar que los controles adecuados están implementados?**
    - **Controles de acceso físico** Se cierran las puertas y se comprueba que no haya nadie en el edificio antes de cerrar.
    - **Alarmas de intrusión** Si, se activan las alarmas.
    - **Monitoreo de CCTV (verificar la retención y frecuencia de revisión)** De vez en cuando.
    - **Se prohíbe el uso de equipos fotográficos, video, audio u otro tipo de grabación** No.
    - **Políticas, procedimientos y pautas** Si, la empresa de seguridad se encarga de actualizar los controles en caso de que sea necesario cada cierto tiempo.

- **¿Cómo se asegura que la información de carácter sensible permanece confidencial a personal autorizado?** La información física es guardada bajo llave y la digital en los servidores de la empresa (solo es posible acceder con usuarios con privilegios).

RESULTADO	COMENTARIO
ADMINISTRADO	Las políticas y la seguridad física se encuentran muy bien definidas

A11.1.6 Áreas de carga y descarga

- **¿Las entregas se hacen en un área segura con control de acceso y limitado a personal autorizado?** Si, las descargas y cargas se realizan con personal autorizado de la empresa.
- **¿Se verifica que el material recibido coincide con un número de pedido autorizado?** Si.
- **¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?** Si.

RESULTADO	COMENTARIO
ADMINISTRADO	Los procesos de recepción y envíos de mensajería los tienen definidos, incluyendo registros de las transacciones. Se siguen las políticas de seguridad establecidas en la organización.

A11.2 Seguridad de los equipos

A11.2.1 Emplazamiento y protección de equipos

- **¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas?** Si, se encuentran en el despacho del departamento.
- **¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada?** Si, se encuentran en los despachos dispuestos para no ser visualizados desde la entrada de la habitación.
- **¿Existen controles para minimizar los siguientes riesgos de amenazas físicas y medioambientales?** -
    - **Agua / inundación** No
    - **Fuego y humo** Si
    - **Temperatura, humedad y suministro eléctrico** Si
    - **Polvo** No
    - **Rayos, electricidad estática y seguridad del personal** No

- **¿Se prueban estos controles periódicamente y después de cambios importantes?** Si, siempre que los equipos tienen que moverse de lugar, el departamento de informática intenta situar los equipos de tal forma que sea complicado espiar desde la puerta.

RESULTADO	COMENTARIO
ADMINISTRADO	La empresa ha tenido ciertos problemas con el agua en el pasado, pero actualmente ya se encuentra todo arreglado y cuenta con una buena protección de los equipos.

A11.2.2 Instalaciones de suministro

- **¿El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad?** Si.
- **¿Hay una capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente?** Si, cada despacho cuenta con uno o más SAI.
- **¿Hay un plan de mantenimiento pare los UPS y generadores en acuerdo con las especificaciones del fabricante?** Si, cada cierto tiempo se cambian las baterías.
- **¿Son probados con regularidad?** Si.
- **¿Hay una red de suministro eléctrico redundante?** No.
- **¿Se realizan pruebas de cambio?** No.
- **¿Se ven afectados los sistemas y servicios?** No.
- **¿Hay sistemas de aire acondicionado para controlar entornos con equipos críticos?** Si.
- **¿Están ubicados apropiadamente?** Si, en el CPD.
- **¿Hay una capacidad adecuada de A / C para soportar la carga de calor?** Si.
- **¿Hay unidades redundantes, de repuesto o portátiles disponibles?** Si, se tienen algunos equipos, discos duros y periféricos de reserva.
- **¿Hay detectores de temperatura con alarmas de temperatura?** No.

RESULTADO	COMENTARIO
ADMINISTRADO	El departamento de informática ha tenido en cuenta la necesidad de instalar SAI en todos sus equipos para prevenir posibles bajadas de tensión eléctrica y tiene en cuenta que la sala de servidores debe estar debidamente refrigerada.

A11.2.3 Seguridad del cableado

- **¿Hay protección física adecuada para cables externos, cajas de conexiones?** Si, la empresa cuenta con cableado interno en las paredes.
- **¿Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias?** Si, los diferentes tipos de cabes se encuentran separados.
- **¿Se controla el acceso a los paneles de conexión y las salas de cableado?** No.
- **¿Existen procedimientos adecuados para todo ello?** No.

RESULTADO	COMENTARIO
REPETIBLE	La instalación del cableado es correcta, pero los paneles de conexión no cuentan con seguridad.

A11.2.4 Mantenimiento de los equipos

- **¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios, HVAC, control de acceso, CCTV, etc.)?** Si.
- **¿Hay programas de mantenimiento y registros / informes actualizados?** Una vez al año.
- **¿Se aseguran los equipos?** Si, cuentan con el seguro de la empresa.

RESULTADO	COMENTARIO
ADMINISTRADO	El mantenimiento se realiza de forma profesional y periódicamente.

A11.2.5 Retirada de materiales propiedad de la empresa

- **¿Existen procedimientos relativos al traslado de activos de información?** No.
- **¿Hay aprobaciones o autorizaciones documentadas en los niveles apropiados?** No.
- **¿Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo?** No.
- **¿Existe un procedimiento para rastrear movimientos de activos de alto valor o alto riesgo?** Si, en estos casos, cuentan con localizadores GPS.

RESULTADO	COMENTARIO
INICIAL	La empresa no cuenta con procedimientos de retirada de activos de la información. Todo se realiza de forma manual e informal.

A11.2.6 Seguridad de los equipos fuera de las instalaciones

- **¿Existe una "política de uso aceptable" que cubra los requisitos de seguridad y "obligaciones" con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas?** -
- **¿Contempla el almacenamiento seguro de los dispositivos, uso cifrado y uso de conexiones seguras?** El uso de conexiones seguras es configurado en los dispositivos por el departamento de informática.
- **¿Existen controles para asegura todo esto?** Si, el departamento de informática evalúa los dispositivos portátiles que se conectan de forma remota a la empresa.
- **¿Cómo se les informa a los trabajadores sobre sus obligaciones?** El departamento de recursos humanos les informa de todo.
- **¿Se les da suficiente apoyo para alcanzar un nivel aceptable de seguridad?** Si

RESULTADO	COMENTARIO
DEFINIDO	**Los dispositivos de trabajadores que requieren trabajar desde casa o forma remota, son configurados por los responsables del departamento de informática.**

A11.2.7 Reutilización o eliminación segura de equipos

- **¿Cómo evita la organización que se revele la información almacenada en equipos tras su reasignación o eliminación?** Se realiza siempre un formateo de los equipos al ser reasignados o eliminados.
- **¿Se utiliza cifrado fuerte o borrado seguro?** Se utiliza un borrado estándar para los equipos de usuario y un borrado a bajo nivel para los discos que contienen información sensible (como los servidores).
- **¿Se mantienen registros adecuados de todos los medios que se eliminan?** No.
- **¿La política y el proceso cubren todos los dispositivos y medios de TIC?** Solo los necesarios.

RESULTADO	COMENTARIO
ADMINISTRADO	**La empresa tiene constancia de la importancia de eliminar la información de sus dispositivos al darlos de baja o reutilizarlos.**

A11.2.8 Equipo de usuario desatendido

- **¿Se suspenden / finalizan las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción?** Si, cuando se detecta cierto tiempo de inactividad, algunas de las aplicaciones de finalizan.
- **¿Se define un tiempo de inactividad adecuado los riesgos de acceso físico no autorizado?** Si, entre 5 y 10 minutos.
- **¿Se protegen los bloqueos de pantalla con contraseña?** Si.
- **¿Se aplica a todos los servidores, equipos de trabajo, portátiles, teléfonos y otros dispositivos TIC?** Si.
- **¿Cómo se verifica el cumplimiento?** Se comprueba cada cierto tiempo.

RESULTADO	COMENTARIO
ADMINISTRADO	Los equipos están configurados para apagar la pantalla tras varios minutos de inactividad y al reconectar aparecerá la pantalla de acceso

A11.2.9 Política de puesto de trabajo despejado y pantalla limpia

- **Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas?** Política como tal no, pero desde gerencia sí que se avisa de que las zonas de trabajo deben estar limpias y despejadas.
- **¿Funciona en la práctica?** En la mayoría de casos.
- **¿Todos los dispositivos informáticos tienen un salvapantallas o bloqueo con contraseña que los empleados usan cuando se alejan de sus dispositivos?** Si, aunque algunos empleados no lo usan.
- **¿Se activa automáticamente tras de un tiempo inactivo definido?** Si.
- **¿Se mantienen las impresoras, fotocopiadoras, escáneres despejados?** Si.

RESULTADO	COMENTARIO
DEFINIDO	Aunque no existe una política como tal, desde gerencia se tiene en consideración que el empleado tenga un entorno de trabajo limpio y despejado.

A12 Seguridad de las operaciones

A12.1 Procedimientos y responsabilidades operacionales

A12.1.1 Documentación de procedimientos operacionales

- **¿Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.?** Si, aunque no está documentado, depende de la forma de trabajar del departamento de IT.
- **¿Existe un conjunto completo de procedimientos de seguridad y cuándo se revisaron por última vez?** Se realiza cada vez que se modifica algún componente en la seguridad, pero no se ha actualizado desde hace varios años.
- **¿Los procesos son razonablemente seguros y están bien controlados?** Si
- **¿Los roles y responsabilidades están bien definidos y se capacita adecuadamente al personal?** Si, los roles están asignados por departamentos.
- **¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)?** Si, pero por falta de tiempo y recursos no se pueden actualizar a menudo.
- **¿Los procedimientos están siendo revisados y mantenidos rutinariamente, autorizados / ordenados, compartidos y usados?** Cuando hace falta.

RESULTADO	COMENTARIO
REPETIBLE	**Existen procesos establecidos, pero sin documentar. El departamento IT está interesado en formalizarlo, pero no se dispone de tiempo para ello.**

A12.1.2 Gestión de cambios

- **¿Existe una política de gestión de cambios?** No.
- **¿Existen registros relacionados a la gestión de cambios?** Solamente aquellos relacionados con el cambio en el código de los programas realizados por el departamento IT o en el departamento de diseño técnico.
- **¿Se planifican y gestionan los cambios?** No realmente.
- **¿Se evalúan los riesgos potenciales asociados con los cambios?** Se prueba primero antes de realizar las modificaciones en producción.

- **¿Los cambios están debidamente documentados, justificados y autorizados por la administración?** En algunas ocasiones.

RESULTADO	COMENTARIO
REPETIBLE	La gestión de cambios no es controlada, pero se disponen de algunos logs donde queda constancia de estos cambios.

A12.1.3 Gestión de capacidades

- **¿Existe una política de gestión de capacidad?** No
- **¿Existen registros relacionados a la gestión de capacidad?** No
- **¿Incluye aspectos tales como las SLA, seguimiento de las métricas relevantes (ej. uso de la CPU, almacenamiento y errores de página, capacidad de la red, demanda de RAM, la capacidad de aire acondicionado, espacio de rack, la utilización, etc.), alarmas / alertas en niveles críticos, la planificación hacia adelante?** No
- **¿Se basa la prioridad en asegurar el rendimiento y la disponibilidad de servicios críticos, servidores, infraestructura, aplicaciones, funciones en un análisis de riesgos?** No.

RESULTADO	COMENTARIO
INEXISTENTE	No se dispone de ninguna medida de gestión de la capacidad

A12.1.4 Separación de los recursos de desarrollo, prueba y operación

- **¿Se segregan entornos de TIC de desarrollo, prueba y operacionales?** Si, existe un entorno de desarrollo.
- **¿Cómo se logra la separación a un nivel de seguridad adecuado?** Empleando diferentes bases de datos.
- **¿Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)?** No, solo existe una red.
- **¿Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos?** No.
- **¿Cómo se promueve y se lanza el software?** Es desarrollado e implantado por el departamento de informática empleando la infraestructura local de la empresa (el software solamente se encuentra disponible para la intranet de la empresa).

- **¿Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección?** Si.
- **¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros?** Si.
- **¿Se identifica un responsable de garantizar que el software nuevo / modificado no interrumpa las operaciones de otros sistemas o redes?** Si, el responsable del departamento IT.

RESULTADO	COMENTARIO
INICIAL	Se dispone de un entorno de pruebas muy rudimentario.

A12.2 Protección contra el software malicioso (malware)

A12.2.1 Controles contra el código malicioso

- **¿Existen políticas y procedimientos asociados a controles antimalware?** Si
- **¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado?** Solamente el departamento de IT tiene la potestad de instalar software.
- **¿Cómo se compila, gestiona y mantiene la lista y por quién?** Lo administra el departamento de IT.
- **¿Hay controles de antivirus de "escaneado en acceso" y "escaneo programático" en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados / IoT?** Sí, todos los sistemas de la empresa tienen antivirus instalado y actualizado.
- **¿Se actualiza el software antivirus de forma automática?** Si.
- **¿Se general alertas accionables tras una detección?** Si.
- **¿Se toma acción de forma rápida y apropiada para minimizar sus efectos?** Si.
- **¿Cómo se gestionan las vulnerabilidades técnicas?** Estudiando la amenaza para encontrar una forma de solucionarla.
- **¿Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte?** No. El departamento de IT pide que cuando pase algo se les avise.
- **¿Existe un mecanismo de escalación para incidentes graves?** No.

RESULTADO	COMENTARIO
DEFINIDO	Los equipos del grupo empresarial están protegidos con anti-virus, pero aun así no se encuentran completamente a salvo de posibles nuevas amenazas de malware.

A12.3 Copias de seguridad

A12.3.1 Copias de seguridad de la información

- **¿Existen políticas y procedimientos asociados a las copias de seguridad?** Si, existen procedimientos empleados por el departamento de IT.
- **¿Existe un mandato basado en el riesgo para un registro preciso y completo de copias de seguridad cuya política de retención y frecuencia reflejen las necesidades del negocio?** Si, se ha establecido en los activos de mayor prioridad.
- **¿Las copias de seguridad cubren los datos y metadatos, sistema y programas de aplicación y los parámetros de configuración de copias de seguridad para todos los sistemas, incluyendo servidores, ordenadores de sobremesa, teléfonos / sistemas de red, sistemas de gestión de red, portátiles, sistemas de control, sistemas de seguridad, etc.?** Se cubre la gran mayoría de los dispositivos.
- **¿Los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales?** Si, se encuentran protegidos como los medios originales.
- **¿Las copias de seguridad se almacenan en ubicaciones adecuadas, protegiendo contra desastres físicos y acceso indebido?** Si, se guardan en una localización externa a la empresa.
- **¿Se mantienen copias off-line para evitar una propagación de ransomware catastrófica?** Si, se tienen copias de seguridad fuera de línea, ya que ha habido experiencias con ransomware.
- **¿Las copias de seguridad se prueban regularmente para garantizar que puedan restaurar?** Si, cada trimestre.
- **¿Hay una clara adherencia a principios de confidencialidad, integridad y disponibilidad?** Si.

RESULTADO	COMENTARIO
ADMINISTRADO	Se realizan copias de toda la información incluida en los servidores de la empresa de forma incremental diariamente.

A12.4 Registros y supervisión

A12.4.1 Registro de eventos

- **¿Existen políticas y procedimientos para el registro de eventos?** Solo procedimientos para cuando hay algún fallo en algún programa.
- **¿Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí?** El registro se basa en logs, pero algunos de los dispositivos envían alertas por correo cuando se detectan incidencias.
- **¿Se registra lo siguiente?** -
    - **cambios en los ID de usuario** No
    - **permisos y controles de acceso** Solo si son externos
    - **actividades privilegiadas del sistema** No
    - **intentos de acceso exitosos y fallidos** Los fallidos
    - **inicio de sesión y cierre de sesión** Solo para conexiones a programas
    - **identidades y ubicaciones de dispositivos** Para los más importantes
    - **direcciones de red, puertos y protocolos** No
    - **instalación de software** No
    - **cambios a las configuraciones del sistema** No
    - **uso de utilidades y aplicaciones del sistema** Si
    - **archivos accedidos y el tipo de acceso** No
    - **filtros de acceso web** No
- **¿Quién es responsable de revisar y hacer un seguimiento de los eventos informados?** El responsable del departamento de informática.
- **¿Cuál es el periodo de retención de eventos?** Una semana.
- **¿Existe un proceso para revisar y responder adecuadamente a las alertas de seguridad?** Cuando surge una alerta de seguridad se revisan los logs.

RESULTADO	COMENTARIO
INICIAL	Se realiza un registro básico de eventos, pero no se suelen comprobar salvo cuando hay un incidente.

A12.4.2 Protección de la información del registro

- **¿Los registros se almacenan / archivan en un formato seguro o mecanismo de control no-editable?** En logs en los servidores.
- **¿El acceso a los registros es adecuadamente controlado, autorizado y monitoreado?** Solo el departamento de informática tiene acceso a ellos.
- **¿Quién tiene o podría obtener acceso a leer / escribir / eliminar registros de eventos?** Los responsables del departamento de informática.
- **¿Hay suficiente capacidad de almacenamiento dado el volumen de registros que se generan y los requisitos de retención?** En ocasiones no.
- **¿Existen copias de seguridad de los registros?** No.

RESULTADO	COMENTARIO
REPETIBLE	No se tiene demasiada consideración por la protección de los logs

A12.4.3 Registros de administración y operación

- **Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos (SIEM)?** No
- **¿Cómo se recogen, almacenan y aseguran, analizan los registros?** De forma manual.
- **¿Existen limitaciones a la capacidad de dichas personas para interferir con los registros o, al menos, no sin generar alarmas de seguridad?** Es realizado por los responsables del departamento de informática.

RESULTADO	COMENTARIO
INICIAL	Actualmente, todo lo relativo a revisión de registros se realiza de forma manual por los responsables del departamento de informática

A12.4.4 Sincronización del reloj

- **¿Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión?** Si
- **¿Hay un tiempo de referencia definido (ej. Reloj atómicos, GPS o NTP)?** NTP
- **¿El método para sincronizar relojes con la referencia cumple con los requisitos comerciales, de seguridad, operacionales, legales, regulatorios y contractuales?** Si

- **¿Está implementado en todo el entorno TI, incluidos los sistemas de monitoreo tales como CCTV, sistemas de alerta, mecanismos de control de acceso, sistemas de auditoría y registro, etc.?** En la mayor parte de ellos
- **¿Existe una configuración de respaldo para la referencia de tiempo?** Si

RESULTADO	COMENTARIO
ADMINISTRADO	Todos los sistemas están sincronizados

A12.5 Control del software en explotación

A12.5.1 Instalación del software en explotación

- **¿Existe una política acerca de la instalación de software?** Si.
- **¿Se asegura que todo software instalado es probado, aprobado, permitido y mantenido para su uso en producción?** Es evaluado por el departamento de informática.
- **¿Se verifica que ya no se utiliza software sin soporte (firmware, sistemas operativos, middleware, aplicaciones y utilidades)?** En la mayor parte.
- **¿Se hace esta verificación en ordenadores de sobremesa, portátiles, servidores, bases de datos, etc.?** Si.
- **¿Existen controles para evitar instalaciones de software, excepto por administradores capacitados y autorizados?** Si.
- **¿Existe un monitoreo y alerta para detectar instalaciones de software no aprobadas?** No.
- **¿Existe un control de cambio y aprobación adecuado para la aprobación de software?** No.

RESULTADO	COMENTARIO
DEFINIDO	**Solamente los técnicos del departamento de informática tienen permisos para la instalación de software.**

A12.6 Gestión de la vulnerabilidad técnica

A12.6.1 Gestión de las vulnerabilidades técnicas

- **¿Existe una política la gestión de vulnerabilidades técnicas?** No.

- **¿Cómo se escanean los sistemas para detectar vulnerabilidades de forma automatizada?** No se hace.
- **¿Cómo responde la organización ante vulnerabilidades técnicas descubiertas en equipos, servidores, aplicaciones, dispositivos de red y otros componentes?** Se reparan.
- **¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes?** No.
- **¿Se ha realizado una evaluación integral de riesgos de los sistemas TIC?** No.
- **¿Se han identificado los riesgos y se han tratado apropiadamente, se han priorizado según el riesgo?** No.
- **¿Se identifican cambios tales como amenazas emergentes, vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución?** Si, cuando surge una amenaza nueva, se comprueban los sistemas.
- **¿Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados? ¿Los procesos para implementar parches urgentes son adecuados?** En ocasiones.
- **¿Se emplea una administración automatizada de parches?** No.
- **¿Existen registros de aprobación o rechazo de implementación de parchas asociado a vulnerabilidades (aceptación de riesgo) en los niveles de administración adecuados?** No.

RESULTADO	COMENTARIO
INICIAL	**Solo se aplican los parches de seguridad siempre que aparece una nueva amenaza de gran riesgo.**

A12.6.2 Restricción en la instalación de software

- **¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados?** Si.
- **¿Los privilegios de instalación están divididos en categorías y permiten instalar tipos de sistemas específicos?** Si.
- **¿Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.?** Si.

RESULTADO	COMENTARIO
ADMINISTRADO	Solamente el personal del departamento de informática puede realizar instalaciones o actualizaciones de software en la empresa.

A12.7 Consideraciones sobre la auditoria de sistemas de información

A12.7.1 Controles de auditoría de sistemas de información

- **¿Existe una política que requiera auditorias de seguridad de la información?** Si.
- **¿Existe un programa definido y procedimientos para auditoría?** Si.
- **¿Las auditorías se planifican cuidadosamente y se acuerdan para minimizar el riesgo de interrupciones en los procesos comerciales?** Si.
- **¿Se define el alcance de la auditoría en coordinación con la administración?** Si.
- **¿El acceso a las herramientas de auditoría de sistemas están controladas para evitar el uso y acceso no autorizado?** Si.

RESULTADO	COMENTARIO
INICIAL	Las auditorias que se han realizado han resultado ser muy básicas y apenas se ha abordado la seguridad de los sistemas de la información.

A13 Seguridad de las comunicaciones

A13.1 Gestión de la seguridad de las redes

A13.1.1 Controles de red

- **¿Existen políticas de redes físicas e inalámbricas?** Existen procedimientos no documentados.
- **¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red?** No.
- **¿Existe un mecanismo de registro i monitorización de la red y los dispositivos que se conectan ella?** Si, aunque son logs.
- **¿Hay un sistema de autenticación para todos los accesos a la red de la organización?** Si.
- **¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos?** Si.

- **¿Los usuarios se autentican adecuadamente al inicio de sesión?** Si, usando el usuario y la contraseña personales.
- **¿Cómo se autentican los dispositivos de red?** Mediante MAC.
- **¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.?** Si, se dispone de una red empresarial y una red de invitados.
- **¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?** Si.

RESULTADO	COMENTARIO
DEFINIDO	**El responsable de redes del departamento de informática ha dispuesto de controles en los dispositivos de acceso al medio.**

A13.1.2 Seguridad de los servicios de red

- **¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada?** Si.
- **¿Existe un monitoreo de servicios de red?** Solo de los esenciales.
- **¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)?** Si.
- **¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red?** Si.
- **¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM?** Cuando el departamento lo requiere.

RESULTADO	COMENTARIO
DEFINIDO	**Los servicios de red se encuentran protegidos. Aunque no se suele monitorizar.**

A13.1.3 Segregación en redes

- **¿Existe una política de segmentación de red?** Si
- **¿Qué tipo de segmentación existe?** Separación de la red en una red privada y una red pública para dispositivos externos o visitas.
- **¿Es basada en la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.)?** En niveles de confianza.
- **¿Cómo se monitorea y controla la segregación?** El router está configurado para ello.
- **¿Se segmenta la red inalámbrica de la red física? ¿Y la red de invitados?** Si.
- **¿Hay controles adecuados entre ellos?** Si.

- **¿Cómo se controla la segmentación con proveedores y clientes?** Se controla mediante las MAC y el rango de IPs.
- **¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?** Si.

RESULTADO	COMENTARIO
DEFINIDO	**La red cuenta con una segregación de la red para distinguir la red privada empresarial de la red para invitados o clientes.**

A13.2 Intercambio de información

A13.2.1 Políticas y procedimientos de intercambio de información

- **¿Existen políticas y procedimientos relacionados con la transmisión segura de información?** No.
- **¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.?** No.
- **¿Está basado en la clasificación de la información?** No.
- **¿Existen controles de acceso adecuados para esos mecanismos?** No.
- **¿Cómo se implementa el uso de criptografía para los mecanismos aceptados (ej. TLS, cifrado de correo electrónico, ZIP codificados)?** No se emplea criptografía.
- **¿Se sigue el principio de confidencialidad y privacidad?** No.
- **¿Existen un programa de concientización, capacitación y cumplimiento?** No.

RESULTADO	COMENTARIO
INICIAL	**El intercambio de información se realiza por correo electrónico. Es la empresa encargada del servicio de correo la que realiza la encriptación de los mensajes.**

A13.2.2 Acuerdos de intercambio de información

Más allá de A.13.2.1

- **¿Qué tipos de comunicaciones se implementan las firmas digitales?** No se aplica.

- **¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos?** Sanciones a nivel de recursos humanos
- **¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas?** No
- **¿Cómo se mantiene una cadena de custodia para las transferencias de datos?** No existe.

RESULTADO	COMENTARIO
INICIAL	El intercambio de información digital se realiza de forma informal.

A13.2.3 Mensajería electrónica

- **¿Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.?** No
- **¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)?** Si
- **¿Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos?** -

RESULTADO	COMENTARIO
DEFINIDO	El intercambio de mensajería electrónica se gestiona por la empresa proveedora del servicio de correo electrónico.

A13.2.4 Acuerdos de confidencialidad o no revelación

- **¿Existen acuerdos de confidencialidad?** Si.
- **¿Han sido revisados y aprobados por el Departamento Legal?** Si.
- **¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)?** Cada vez que se actualiza la ley.
- **¿Han sido aprobados y firmados por las personas adecuadas?** Si.
- **¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?** Si.

RESULTADO	COMENTARIO
DEFINIDO	Existen acuerdos de confidencialidad que pretenden proteger la información sensible de la empresa.

A14 Adquisición, desarrollo y mantenimiento de los sistemas de información

A14.1 Requisitos de seguridad en los sistemas de información

A14.1.1 Análisis de requisitos y especificaciones de seguridad de la información

- **¿Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software?** Se evalúa la seguridad cada vez que se va a implantar un nuevo sistema o software, pero no existe un procedimiento como tal.
- **¿Existen procedimientos para analizar riesgos, requisitos funcionales y técnicos, arquitectura de seguridad, las pruebas de seguridad y la certificación de sistemas y desarrollo?** No existen procedimientos, los análisis se realizan de forma informal.
- **¿Son estos procedimientos obligatorios para todos los nuevos desarrollos y cambios en los sistemas existentes (ej. Actualizaciones de sistema operativo / aplicaciones en las actualizaciones, cambios de criptografía, etc.)** No.
- **¿Se aplican estos controles para sistemas / software comercial, incluidos los productos "a medida" o personalizados?** Solo al realizar la implantación.

RESULTADO	COMENTARIO
INICIAL	Se realizan evaluaciones de seguridad de los nuevos componentes hardware o software, pero de manera informal.

A14.1.2 Asegurar los servicios de aplicaciones en redes públicas

- **¿La organización usa o proporciona aplicaciones web de comercio electrónico?** -
- **¿Se verifican los aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y la disponibilidad del servicio?** -
- **¿Contiene controles tales como validación de datos de entrada, validación de procesamiento, encriptación, autenticación de mensajes e irrenunciabilidad?** -
- **¿Se fuerza https?** -
- **¿Los sitios web públicos están siendo monitoreados (ej. eventos, vulnerabilidades, etc.)?** -
- **¿Se analizan y documentan las amenazas de forma rutinaria?** -
- **¿Existe una gestión de incidentes y cambios para tratarlos?** –

RESULTADO	COMENTARIO
OPTIMIZADO	La empresa ofrece un portal web de forma pública. Este portal web se encuentra diseñado y administrado por una empresa externa.

A14.1.3 Protección de las transacciones de servicios de aplicaciones

Más allá de A.14.1.2

- **¿Las transacciones se realizan y almacenan en un entorno interno seguro o expuesto a internet?** -
- **¿Se protege la información mediante el uso de protocolos seguros, cifrado, firma electrónica, etc.?** -
- **¿Cumplen con todos los requisitos legales, regulatorios y de cumplimiento?** –

RESULTADO	COMENTARIO
NO APLICABLE	La empresa no ofrece servicios de aplicaciones

A14.2 Seguridad en el desarrollo y en los procesos de soporte

A14.2.1 Política de desarrollo seguro

- **¿Existe una política de desarrollo seguro que abarque la arquitectura de seguridad?** No.
- **¿Los entornos de desarrollo usan repositorios seguros con control de acceso, seguridad y control de cambios?** Si.
- **¿Los métodos de desarrollo incluyen pautas de programación segura?** No.
- **¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?** No.

RESULTADO	COMENTARIO
INICIAL	Actualmente, en la empresa no se tiene demasiado en cuenta la seguridad en sus desarrollos.

A14.2.2 Procedimiento de control de cambios en sistemas

- **¿Existen políticas, procedimientos y registros relacionados de la gestión de cambios?** No.

- **¿Incluyen planificación y prueba de cambios, evaluaciones de impacto (incluido el riesgo de información y aspectos de seguridad, más los impactos de no cambiar), verificaciones de instalación y procedimientos de retroceso / reversión?** No
- **¿Incluye un procedimiento para cambios de emergencia?** No.
- **¿Se aplica los cambios significativos en equipos informáticos y de telecomunicaciones?** No.
- **¿Los cambios en el sistema están debidamente documentados, justificados y autorizados por la administración?** Solo si son cambios de naturaleza critica.

RESULTADO	COMENTARIO
INEXISTENTE	No existe un procedimiento de control de cambios en sistemas.

A14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

- **¿Se requiere una validación / evaluaciones de riesgo y, si es necesario, recertificación de sistemas tras actualizaciones / mantenimiento, parches, cambios sistema operativo, actualizaciones de aplicaciones y cambios de cifrado?** Solamente si se detecta un nuevo problema.
- **¿Hay registros de estas actividades?** No.

RESULTADO	COMENTARIO
INICIAL	La revisión de las aplicaciones tras los cambios las suele realizar el propio administrador de sistemas.

A14.2.4 Restricciones a los cambios en los paquetes de software

- **¿Se hacen cambios a paquetes software adquiridos?** Si, si la empresa lo requiere como es el caso del ERP Navision 2018.
- **¿Se verifica que los controles originales no han sido comprometidos?** Si
- **¿Se obtuvo el consentimiento y la participación del proveedor?** Si, el proveedor además da soporte para ayudar a realizar los cambios.
- **¿El proveedor continúa dando soporte tras los cambios?** Si
- **¿Se exploró la posibilidad de obtener actualizaciones de programas estándar por parte de los proveedores?** Si
- **¿Se hace una comprobación de compatibilidad con otro software en uso?** Si.

RESULTADO	COMENTARIO
ADMINISTRADO	Solamente se realizan cambios en paquetes de software que permitan esos cambios y siempre con la ayuda de los partners.

A14.2.5 Principios de ingeniería de sistemas seguros

- **¿Se siguen principios de SDLC que incluye controles de seguridad?** No.
- **¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?** No.

RESULTADO	COMENTARIO
INEXISTENTE	No se ha tenido en cuenta hasta ahora la inclusión de seguridad en los desarrollos de la empresa.

A14.2.6 Entorno de desarrollo seguro

- **¿Se aíslan los entornos de desarrollo?** No.
- **¿Cómo se desarrolla, prueba y lanza el software?** Se realiza en el departamento de informática y se prueba en los propios sistemas de los desarrolladores.
- **¿Quién es responsable de garantizar que el software nuevo / modificado no interrumpa otras operaciones?** El propio desarrollador.
- **¿Se realizan comprobaciones de antecedentes de los desarrolladores?** No.
- **¿Tienen que cumplir con un NDA?** No.
- **¿Cuáles son los reglamentos y los requisitos de cumplimiento que afectan el desarrollo?** Que funcione tal como se pide.
- **¿Cómo se protegen los datos de prueba de la divulgación y dónde están almacenados?** No se protegen. Se encuentran en los propios equipos de los desarrolladores.

RESULTADO	COMENTARIO
INICIAL	El desarrollo se realiza de manera informal.

A14.2.7 Externalización del desarrollo de software

Más allá de A.14.2.6

- **¿Se tienen en cuanta los siguientes aspectos cuando el desarrollo es lleva a cabo por un tercero?**

- **Los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual** Sí.
- **Requisitos contractuales para prácticas seguras de diseño, desarrollo y prueba** No.
- **Acceso al código fuente si el código ejecutable necesita ser modificado** Sí.
- **Controles de prueba de seguridad de aplicaciones** A veces.
- **Evaluación de vulnerabilidad y tratamiento** No.

RESULTADO	COMENTARIO
INEXISTENTE	Los desarrollos realizados por empresas externas no suelen tener en cuenta la seguridad.

A14.2.8 Pruebas funcionales de seguridad de sistemas

Más allá de A.14.2.7

- **¿Existe un procedimiento de pruebas y verificación para sistemas nuevos y actualizados?** Se prueban los sistemas nuevos de manera informal.
- **¿Tiene en cuenta acuerdos de licencia, propiedad del código y propiedad intelectual?** Si

RESULTADO	COMENTARIO
REPETIBLE	Se realizan pruebas de funcionamiento y se observa cómo afecta a los servidores.

A14.2.9 Pruebas de aceptación de sistemas

- **¿Se efectúan pruebas de seguridad antes de la introducción de nuevos sistemas en la red?** Si.
- **¿Las pruebas replican situaciones y entornos operativos realistas?** Si.
- **¿Los defectos relacionados con la seguridad son tratados antes de que el producto sea certificado / aprobado?** Si.
- **¿Hay pruebas de aceptación del usuario (UAT) antes del lanzamiento al entorno operativo?** No.
- **¿Se actualizan los controles de resiliencia y recuperación tras incidentes para reflejar los sistemas nuevos, modificados y retirados?** No.

RESULTADO	COMENTARIO
DEFINIDO	Siempre que hay un nuevo sistema en la red, se comprueba la estabilidad de todo el conjunto.

A14.3 Datos de prueba

A14.3.1 Protección de los datos de prueba

- **¿Se utilizan mecanismos para proteger datos de prueba como la seudonimización, enmascaramiento, datos falsos, borrado, etc.?** No.
- **¿Existe un mecanismo de verificación y aprobación para el uso de datos no protegidos para pruebas?** No
- **¿Existen registros de estas actividades?** No

RESULTADO	COMENTARIO
INEXISTENTE	Los datos de prueba son generados usando copias de seguridad de días anteriores, por lo que son datos verdaderos.

A15 Relación con proveedores

A15.1 Seguridad en las relaciones con proveedores

A15.1.1 Política de seguridad de la información en las relaciones con los proveedores

- **¿Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI?** Si
- **¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo?** Si.
- **¿Los contratos y acuerdos abordan lo siguiente?**
    - **Arreglos de gestión de relaciones, incluyendo el riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada** No
    - **Información / propiedad intelectual, y obligaciones / limitaciones derivadas** Si
    - **Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información** No
    - **Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001** No

- **Identificación de controles físicos y lógicos** Si
- **Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio** Si
- **Habilitación de seguridad de los empleados y concienciación** No
- **Derecho de auditoría de seguridad por parte de la organización** En algunos casos

- **¿Existe una obligación contractual de cumplimento?** Si
- **¿Los proveedores de servicios externos son monitoreados rutinariamente y auditados para cumplir con los requisitos de seguridad?** No

RESULTADO	COMENTARIO
ADMINISTRADO	Las relaciones con los proveedores están establecidas mediante contrato y se confía en los servicios que los proveedores pueden ofrecer en cuanto a seguridad.

A15.1.2 Requisitos de seguridad en contratos con terceros

- **¿Los contratos o acuerdos formales con proveedores cubren lo siguiente?**
  - **Gestión de las relaciones, incluyendo riesgos** Si
  - **Cláusulas de confidencialidad vinculantes** Si
  - **Descripción de la información que se maneja y el método de acceder a dicha información** Si
  - **Estructura de la clasificación de la información a usar** Si
  - **La Inmediata notificación de incidentes de seguridad** Si
  - **Aspectos de continuidad del negocio** Si
  - **Subcontratación y restricciones en las relaciones con otros proveedores** Si
  - **Aspectos de personal y RRHH (ej. Rendimiento, antecedentes, "robo de empleados", etc.)** Si

RESULTADO	COMENTARIO
ADMINISTRADO	Los contratos con los proveedores cubren la mayoría de los puntos requeridos por la legislación.

A15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones

Más allá de A.15.1.1 y A.15.1.2

- **¿Cómo se validan los requisitos de seguridad de los productos o servicios adquiridos?** Se comprueban que cumplan con los requisitos especificados por la empresa.
- **¿Cómo se logra una capacidad de recuperación cuando productos o servicios críticos son suministrados por terceros?** Se llama por teléfono a la empresa suministradora para que solucione la incidencia cuanto antes sea posible.
- **¿Se puede rastrear el origen del producto o servicio?** Si.

RESULTADO	COMENTARIO
ADMINISTRADO	Siempre se considera que es indispensable que la empresa suministradora cuente con una línea directa de atención.

A15.2 Gestión de la provisión de servicios del proveedor

A15.2.1 Control y revisión de la provisión de servicios del proveedor

- **¿Existe una monitorización de servicios y quien responsable de esta actividad?** No.
- **¿Se llevan a cabo reuniones de revisión del servicio, con qué frecuencia?** Solo cuando se requiere un nuevo servicio o modificación.
- **¿Se generan informes y / o métricas relacionadas a las reuniones y las decisiones tomadas?** Si, se toman notas.
- **¿Las reuniones abarcan riesgos, incidentes, políticas, cumplimiento e informes de auditoría?** Depende del servicio
- **¿Existen cláusulas de penalización o de bonificación en el contrato relacionadas con el riesgo de la información?** No, la mayoría de veces.

RESULTADO	COMENTARIO
REPETIBLE	Las revisiones de la calidad del servicio solo se realizan cuando se detectan incidentes relacionados.

A15.2.2 Gestión de cambios en la provisión del servicio del proveedor

- **¿Cómo se comunican cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados?** Mediante correo electrónico o teléfono.

- **¿Cómo se comunican cambios en las políticas y requerimientos legales de la organización?** Mediante correo electrónico o teléfono.
- **¿Se actualizan los acuerdos relacionados con los cambios?** Si.

RESULTADO	COMENTARIO
ADMINISTRADO	Se mantiene el contacto directo con los proveedores de servicios.

A16 Gestión de incidentes de seguridad de la información

A16.1 Gestión de incidentes de seguridad de la información y mejoras

A16.1.1 Responsabilidades y procedimientos

- **¿Existen políticas, procedimientos e ITT´s para la gestión de incidentes?** No
- **¿Qué cubre?** -
    - **El plan de respuesta a incidentes** -
    - **Puntos de contacto para la notificación de incidentes, seguimiento y evaluación** -
    - **Monitoreo, detección y reporte de eventos de seguridad** -
    - **Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio** -
    - **Método de recolección de evidencias y pruebas forenses digitales** -
    - **Revisión post-evento de seguridad y procesos de aprendizaje / mejora** -
- **¿Existen evidencias de la notificación de incidentes, registro, clasificación, asignación de resolución, la mitigación y la confirmación de cierre?** No

RESULTADO	COMENTARIO
INICIAL	La gestión de incidentes se realiza de manera informal por el departamento de informática.

A16.1.2 Notificación de los eventos de seguridad de la información

- **¿Cómo se informan los eventos de seguridad de la información?** El departamento de informática avisa enviando correos electrónicos a todos los responsables de departamento.
- **¿Son conscientes los trabajadores de la necesidad de informar de inmediato y lo hacen?** Solo algunos de ellos.

- **¿Se crean informes de seguimiento de los incidentes? Desde la detección a la resolución.** No.
- **¿Qué pasa con esos informes?** -

RESULTADO	COMENTARIO
INICIAL	La notificación de eventos la realiza el departamento de informática y solo cuando algún empleado les ha consultado alguna duda.

A16.1.3 Notificación de puntos débiles de la seguridad

Más allá de A.16.1.2

- **¿Existe una obligación contractual por parte de los empleados para reportar cualquier tipo de ocurrencia inusual?** No.
- **¿Las políticas prohíben explícitamente a los trabajadores 'verificar', 'explorar', 'validar' o 'confirmar' vulnerabilidades a menos que estén expresamente autorizados para hacerlo?** No.

RESULTADO	COMENTARIO
INEXISTENTE	La notificación de puntos débiles de la seguridad es voluntaria.

A16.1.4 Evaluación y decisión sobre los eventos de seguridad de información

- **¿Qué tipos de eventos se espera que informen los empleados?** Funcionamiento erróneo de las aplicaciones del sistema.
- **¿A quién informan?** Al responsable del departamento de informática.
- **¿Cómo se evalúan estos eventos para decidir si califican como incidentes?** Se comentan entre los responsables del departamento IT.
- **¿Hay una escala de clasificación?** Si.
- **¿Hay un proceso de clasificación y / o escalamiento para priorizar los incidentes graves?** Si.
- **¿En qué se basa?** En los sistemas afectados.

RESULTADO	COMENTARIO
REPETIBLE	La evaluación de los eventos de seguridad de la información se realiza entre los miembros del departamento IT, para confirmar la prioridad a seguir.

A16.1.5 Respuesta a incidentes de seguridad de la información

- **¿Cómo se recolecta, almacena y evalúa la evidencia?** Logs y en algunos casos imágenes.
- **¿Hay una matriz de escalación para usar según sea necesario?** No.
- **¿Hay medios para comunicar información de tales incidentes a las organizaciones internas y externas pertinentes?** Mediante el correo electrónico o el teléfono.
- **¿Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente?** Si es de extrema gravedad, sí.

RESULTADO	COMENTARIO
INICIAL	La empresa no tiene apenas experiencia en incidentes de seguridad de la información, por lo que no se ha creado un procedimiento.

A16.1.6 Aprendizaje de los incidentes de seguridad de la información

- **¿Existe un proceso de evaluación / investigación para identificar incidentes de impacto recurrentes?** Si
- **¿Se aprovecha la información obtenida de la evaluación de incidentes para evitar recurrencias?** Si
- **Además, ¿Se está utilizado para formación y concienciación?** No
- **¿La organización cuenta con un proceso de gestión de incidentes relativamente maduro?** No
- **¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?** Si

RESULTADO	COMENTARIO
INICIAL	Cuando ocurre un incidente de seguridad de forma recurrente, esto es analizado para tratar de encontrar la causa y solucionarlo.

A16.1.7 Recopilación de evidencias

- **¿La recolección de evidencias de hace de forma competente en la empresa o por terceros especializados y capacitados en esta área?** -
- **¿Haya personal capacitado, competente y confiable con herramientas adecuadas y procesos definidos para el rol?**

- **(cadena de evidencia rigurosamente mantenida, evidencia asegurada en almacenamiento, herramientas y técnicas)** -
- **¿Quién decide emprender un análisis forense, y en qué criterio se base?** -
- **¿Existen obligaciones relacionadas con la jurisdicción, las diferentes normas forenses y los requisitos legales asociados?** –

RESULTADO	COMENTARIO
INEXISTENTE	Nunca se ha considerado la recopilación de evidencias, pero de hacerse se necesitaría ayuda externa.

A17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio

A17.1 Continuidad de la seguridad de la información

A17.1.1 Planificación de la continuidad de la seguridad de la información

- **¿Cómo se determinan los requisitos de continuidad del negocio?** Por la importancia de los servicios.
- **¿Existe un plan de continuidad de negocio?** No se ha considerado crear un plan de continuidad de negocio en la empresa.
- **¿Existen un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos?** -
- **¿Se identifica el impacto potencial de los incidentes?** -
- **¿Se evalúan los planes de continuidad del negocio?** -
- **¿Se llevan a cabo ensayos de continuidad?** –

RESULTADO	COMENTARIO
INEXISTENTE	No existe un plan de continuidad de la seguridad de la información.

A17.1.2 Implementar la continuidad de la seguridad de la información

- **¿Los planes tienen plazos definidos para restaurar servicios tras una interrupción?** No.
- **¿Los planes tienen en cuenta la identificación y el acuerdo de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares?** No.

- **¿La planificación de la continuidad es consistente e identifica las prioridades de restauración?** No.
- **¿Tienen los miembros de los equipos de recuperación / gestión de crisis / incidentes conocimiento de los planes y tienen claro sus roles y responsabilidades?** No.
- **¿Los controles de seguridad son adecuados en los sitios de recuperación de desastres remotos?** No

RESULTADO	COMENTARIO
INEXISTENTE	

A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

- **¿Existe un método de pruebas del plan de continuidad?** No.
- **¿Con qué frecuencia se llevan a cabo dichas pruebas?** -
- **¿Hay evidencia de las pruebas reales y sus resultados?** -
- **¿Se han identificado deficiencias?, ¿Se han remediado? y ¿Se han vuelto a probar hasta que los resultados sean satisfactorios?** –

RESULTADO	COMENTARIO
INEXISTENTE	

A17.2 Redundancias

A17.2.1 Disponibilidad de los recursos de tratamiento de la información

- **¿Cómo se identifican los requisitos de disponibilidad de servicios?** Realizando una evaluación para comprobar cuáles son los servicios más indispensables que requiere la empresa para su funcionamiento.
- **¿Se tienen en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga?** Si.
- **¿Se tienen en cuenta servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí?** Si.
- **¿Los controles clave de seguridad de la información están implementados y son funcionales en los sitios de recuperación de desastres?** No

RESULTADO	COMENTARIO
ADMINISTRADO	Se tiene en gran consideración la disponibilidad de los activos de información.

A18 Cumplimiento

A18.1 Cumplimiento de los requisitos legales y contractuales

A18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

- **¿Existe una política acerca del cumplimiento de requisitos legales? LOPD, GDPR, etc.** Si, debido al carácter de la empresa se requiere cumplir ciertos requisitos legales.
- **¿Se mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables?** Si.
- **¿Hay una persona encargada de mantener, usar y controlar el registro?** Si.
- **¿Cómo se logra y se garantiza el cumplimiento?** Con ayuda de una empresa externa.
- **¿Existen controles adecuados para cumplir con los requisitos?** Si

RESULTADO	COMENTARIO
OPTIMIZADO	La empresa se basa en las normativas y leyes para cumplir con la legislación. Una vez al año, se requiere la participación de una empresa externa consultora que garantiza el cumplimiento de los requisitos legales.

A18.1.2 Derechos de Propiedad Intelectual (DPI)

- **¿Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento?** Si

RESULTADO	COMENTARIO
OPTIMIZADA	El departamento de informática solo tiene permitido la instalación de software legal.

A18.1.3 Protección de los registros de la organización

- **¿Existe una política que contemple lo siguiente? Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos.** No.
- **¿Se almacenan las firmas digitales de forma segura?** Si.

- **¿Se contempla la posibilidad de destrucción, falsificación y acceso no autorizado?** Si.
- **¿Se verifica periódicamente la integridad de los registros?** No.
- **¿Se utilizan medios de almacenamiento de larga duración para el almacenamiento a largo plazo?** Si.

RESULTADO	COMENTARIO
DEFINIDO	**Los registros más importantes de la empresa se encuentran protegidos en zonas donde solo los roles con mayores privilegios pueden acceder. Pero carece de una política que lo contemple.**

A18.1.4 Protección y privacidad de la información de carácter personal

- **¿Hay un mecanismo para instruir al personal en el manejo de información de carácter personal?** Si.
- **¿Hay un responsable de privacidad en la organización?** Si.
- **¿Es el responsable conocedor de la información de carácter personal que es recopilado, procesado y almacenados por la organización?** Si.
- **¿Cuáles son los controles de acceso a información de carácter personal?** Mediante roles de usuario.
- **¿Cuál es el nivel de acceso y roles (de personal) que tienen acceso a estos activos?** Administradores y recursos humanos.

RESULTADO	COMENTARIO
ADMINISTRADO	**La información de carácter personal es administrada por el personal de recursos humanos.**

A18.1.5 Regulación de los controles criptográficos

- **¿Existe una política que cubra actividades relacionadas con importación / exportación de material criptográfico?** No.
- **¿Estas actividades cumplen con los requisitos legales y reglamentarios?** –

RESULTADO	COMENTARIO
INEXISTENTE	**Los controles criptográficos no están regulados.**

A18.2 Revisiones de la seguridad de la información

A18.2.1 Revisión independiente de la seguridad de la información

- **¿Están las prioridades de implementación de controles alineadas con los riesgos a activos de información?** No.
- **¿Los requisitos de auditoría de sistemas son cuidadosamente planificados, autorizados, implementados y controlados para minimizar los riesgos?** No.
- **¿Están los objetivos y el alcance de auditoria autorizados por la gerencia?** No.
- **¿Está adecuadamente controlado el acceso a las herramientas / software de auditoría del sistema de información?** No.
- **¿Se documentan los hallazgos de auditoría y las actuaciones para solventarlos?** –

RESULTADO	COMENTARIO
INICIAL	No se suelen hacer revisiones de la seguridad de la información.

A18.2.2 Cumplimiento de las políticas y normas de seguridad

- **¿Cómo garantizar que todos los procedimientos de seguridad dentro de un área de responsabilidad se llevan a cabo correctamente?** No se puede garantizar.
- **¿Se hace una verificación periódica?** No

RESULTADO	COMENTARIO
INICIAL	No se puede garantizar un cumplimiento de las políticas y normas de seguridad por los empleados de la empresa.

A18.2.3 Comprobación del cumplimiento técnico

- **¿Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting?** No.
- **¿Las pruebas son realizadas por profesionales debidamente cualificados y confiables?**
- **¿Cómo informa, analiza y utilizan los resultados de dichas pruebas?** -
- **¿La prioridad de tratamiento se basa en un análisis de riesgos?** -
- **¿Hay evidencias de medidas tomadas para abordar los problemas identificados?** –

RESULTADO	COMENTARIO
INEXISTENTE	No se realiza ninguna clase de comprobación del cumplimiento técnico.

Anexo II – Inventario de activos – Fichas detalle

- [D] Datos / Información

Código: D001	**Nombre:** Documentación y datos de la producción	
Descripción: Documentos y planos referentes a los productos de la fabricación, incluyendo instrucciones para producir los productos.		
Propietario: Responsable Producción		**Responsable:** Gerente
Tipo: [files]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La no disponibilidad de datos de producciones afectara muy negativamente a las fabricaciones
[I]	A	La modificación de datos de producciones podría afectar negativamente a las fabricaciones
[C]	A	La fuga de esta información afectaría directamente a negocio
[A]	MA	Es importante que los datos sean reales para que el éxito del negocio tenga efecto
[T]	MA	La trazabilidad de acceso a los datos es importante para el análisis de fugas de información
Total	MA	Los datos de los productos son realmente importantes para la correcta y continua producción de la empresa
Dependencias de activos inferiores		
Activo: ERP (Microsoft Dynamics Navision 2017)		**¿Por qué?** La información de los productos se guardan en el ERP de la empresa
Activo: NAS		**¿Por qué?** El NAS es el que almacena los planos y procedimientos del proceso de fabricación

Código: D002	**Nombre:** Archivo de clientes
Descripción: Datos de los clientes ubicados en el ERP (Microsoft Dynamics Navision 2017) de la empresa.	
Propietario: Responsable Administración	**Responsable:** Gerente
Tipo: [files]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La no disponibilidad de datos de clientes afectara muy negativamente a la actividad de la empresa
[I]	EX	La modificación de datos de clientes afectaría directamente a negocio
[C]	EX	La fuga de esta información afectaría directamente a negocio
[A]	MA	Es importante que los datos sean reales para que el éxito del negocio tenga efecto
[T]	MA	La trazabilidad de acceso a los datos es importante para el análisis de fugas de información
Total	EX	Los datos de los clientes son indispensables para el día a día de la empresa y sus relaciones comerciales

Dependencias de activos inferiores	
Activo: ERP (Microsoft Dynamics Navision 2017)	**¿Por qué?** La información de los clientes se guardan en el ERP de la empresa
Activo: Gestor de proyectos	**¿Por qué?** El gestor de proyectos también dispone de información de los clientes

Código: D003	**Nombre:** Datos de acceso usuarios
Descripción: Credenciales de acceso a los terminales clientes.	
Propietario: Usuario	**Responsable:** Responsable Dpto. Informatica
Tipo: [password]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La no disponibilidad de las credenciales de acceso, impediría al usuario acceder al sistema
[I]	M	La modificación de las credenciales afectaría al usuario
[C]	A	La fuga de esta información podría acarrear accesos no autorizados
[A]	M	Es importante que las credenciales sean reales para el acceso del usuario
[T]	M	La trazabilidad de acceso de los usuarios es importante para el análisis de fugas de información
Total	A	Los datos de los productos son realmente importantes para la correcta y continua producción de la empresa

Dependencias de activos inferiores	
Activo: Active Directory	**¿Por qué?** La información de acceso de los empleados se guardan en Active Directory

Código: D004	**Nombre:** Datos acceso servidor
Descripción: Credenciales de acceso a los servidores.	
Propietario: Responsable TI	**Responsable:** Gerente
Tipo: [password]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La no disponibilidad de las claves de acceso a los servidores afectara muy negativamente a los sistemas de la empresa
[I]	MA	La modificación de las claves de acceso a los servidores dejaría a la empresa sin el control de los servidores
[C]	MA	La confidencialidad de la clave de servidor debe ser de suma importancia
[A]	MA	Es importante que las claves sean reales para que el éxito del negocio tenga efecto.
[T]	M	La trazabilidad de accesos a las cuentas de administración es importante para el análisis de fugas de información
Total	MA	Las claves de acceso a los servidores deben ser muy bien protegidas, ya que se debe proteger la información de la empresa

Código: D005	**Nombre:** Copias de seguridad
Descripción: Copias incrementales de respaldo de los datos de los servidores.	
Propietario: Responsable TI	**Responsable:** Gerente
Tipo: [backup]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad de las copias de seguridad es necesaria en cualquier momento ante cualquier posible imprevisto
[I]	A	La integridad de los datos del backup es necesaria para poder emplear los backups en caso de necesidad
[C]	A	La confidencialidad de los datos del servidor debe ser de suma importancia
[A]	A	Es importante que los datos sean reales para poder emplear los backups en caso de necesidad
[T]	M	La trazabilidad de acceso a los datos de los backups puede ser útil
Total	A	Las copias de seguridad son indispensables para volver a recuperar cualquier tipo de dato de la empresa

Dependencias de activos inferiores	
Activo: Sistema de backup	**¿Por qué?** El sistema de backups es el que se encarga de hacer las copias de seguridad según su programación
Activo: Discos duros extraíbles	**¿Por qué?** Algunos de los backups se realizan ocasionalmente empleando discos duros externos

Código: D006	**Nombre:** Ficheros LOG	
Descripción: Ficheros sobre los que se realiza un registro de actividad de la información		
Propietario: Responsable TI		**Responsable:** Gerente
Tipo: [log]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad de los LOGs puede resultar util en ocasiones
[I]	M	La integridad de los logs es útil para comprobar ciertas acciones
[C]	M	La confidencialidad no es muy necesaria si no se expone información sensible
[A]	M	Es importante que los datos de los logs sean reales
[T]	M	La trazabilidad de acceso a los logs no es demasiado necesaria
Total	A	El registro de LOGs puede ayudar a comprobar ciertas actividades, como errores y accesos no autorizados
Dependencias de activos inferiores		
Activo: Servidor		**¿Por qué?** Los LOGs se almacenan en sus correspondientes servidores

Código: D007	**Nombre:** Ficheros de configuración
Descripción: Ficheros de configuración de las aplicaciones y servicios de la empresa	
Propietario: Responsable TI	**Responsable:** Gerente
Tipo: [conf]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La no disponibilidad de los ficheros de configuración afectara muy negativamente a las aplicaciones
[I]	MA	La modificación de los ficheros de configuración afectaría directamente a negocio
[C]	A	La fuga de esta información afectaría directamente a negocio
[A]	A	Es muy importante que los ficheros de configuración sean auténticos
[T]	MA	La trazabilidad de acceso es indispensable para controlar los cambios en los ficheros de configuración
Total	A	Los ficheros de configuración son de vital importancia para el buen funcionamiento de las aplicaciones y servicios de la empresa

Dependencias de activos inferiores	
Activo: Servidor	**¿Por qué?** Los ficheros de configuración se almacenan y disponen en los servidores

Código: D008	**Nombre:** Base de datos del ERP
Descripción: Fichero de almacenamiento de la Base de Datos dedicada al ERP	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [int]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La no disponibilidad de la base de datos del ERP impedirá que el ERP funcione
[I]	MA	La modificación de datos de ERP afectará negativamente a las fabricaciones
[C]	MA	La fuga de esta información del ERP afectaría directamente a negocio
[A]	MA	Es muy importante que los datos del ERP sean reales para que el éxito del negocio tenga efecto
[T]	MA	La trazabilidad de acceso a los datos es importante para el análisis de fugas de información y posibles errores humanos
Total	MA	Los datos incluidos en el ERP son indispensables para la correcta y continua producción de la empresa

Dependencias de activos inferiores	
Activo: ERP (Microsoft Dynamics Navision 2017)	**¿Por qué?** La base de datos del ERP depende la información introducida en el ERP de la empresa
Activo: Servidor	**¿Por qué?** La base de datos del ERP se almacena en uno de los servidores principales

Código: D009	**Nombre:** Base de datos del Gestor de proyectos
Descripción: Fichero de almacenamiento de la base de datos dedicada al Gestor de proyectos	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [int]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La no disponibilidad de datos de proyectos afectara muy negativamente a la planificación
[I]	MA	La modificación de datos de proyectos afectará negativamente a las planificaciones
[C]	A	La fuga de esta información afectaría directamente a negocio
[A]	MA	Es importante que los datos sean reales para que el éxito del negocio tenga efecto
[T]	A	La trazabilidad de acceso a los datos es importante para el análisis de fugas de información y de errores en la planificación
Total	MA	Los datos incluidos en el gestor de proyectos son indispensables para la planificación de fabricaciones de la empresa

Dependencias de activos inferiores	
Activo: Gestor de proyectos	**¿Por qué?** La información de la base de datos se genera en el gestor de proyectos
Activo: Servidor	**¿Por qué?** La base de datos se almacena en el Servidor

Código: D010	**Nombre:** Datos personal empresa
Descripción: Documentos referentes al personal de la empresa: tal como contratos, nominas…	
Propietario: Recursos humanos	**Responsable:** Gerente
Tipo: [files]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La no disponibilidad de los datos del personal afectará al transcurso de las operaciones cotidianas de la empresa
[I]	A	La modificación de los datos de empleados podría afectar negativamente a la empresa
[C]	EX	La fuga de esta información afectaría directamente a negocio y pondría a la empresa en ciertos problemas legales
[A]	MA	Es importante que los datos sean reales para que el éxito del negocio tenga efecto
[T]	MA	La trazabilidad de acceso a los datos es importante para el análisis de fugas de información
Total	EX	Proteger los datos de los empleados es indispensable para el buen hacer de la empresa y cumplir con la legislación vigente

Dependencias de activos inferiores	
Activo: ERP (Microsoft Dynamics Navision 2017)	**¿Por qué?** El ERP puede generar información referente a los empleados
Activo: Gestor de proyectos	**¿Por qué?** El gestor de proyectos genera información referente a los empleados
Activo: Servidor	**¿Por qué?** La información de los empleados se guardan en el servidor de la empresa

Código: D011	**Nombre:** Diseños	
Descripción: Diseños referentes a los productos de la fabricación		
Propietario: Responsable Diseño		**Responsable:** Gerente
Tipo: [files]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	M	La no disponibilidad de los diseños podría afectar momentáneamente a algunas fabricaciones
[I]	A	La modificación de datos de diseño podría afectar negativamente a las fabricaciones
[C]	A	La fuga de esta información afectaría directamente a negocio
[A]	MB	No se consideran alteraciones de los diseños
[T]	M	Incorporar trazabilidad puede resultar útil
Total	M	La protección de los diseños puede resultar útil en ciertos casos
Dependencias de activos inferiores		
Activo: Suite de diseño grafico		**¿Por qué?** Los diseños se generan empleando este software
Activo: NAS		**¿Por qué?** El NAS es donde se almacenan los diseños

Código: D012	**Nombre:** Mecanizados
Descripción: Programas referentes a los productos de la fabricación, incluyendo instrucciones para que las máquinas produzcan las piezas paso a paso	
Propietario: Responsable Diseño Técnico	**Responsable:** Gerente
Tipo: [exe]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La no disponibilidad de los mecanizados afectara muy negativamente a las fabricaciones
[I]	A	La modificación de datos de mecanizados podría afectar negativamente a las fabricaciones
[C]	A	La fuga de esta información afectaría directamente a negocio
[A]	MA	Es importante que los mecanizados sean reales para que el éxito del negocio tenga efecto
[T]	MA	La trazabilidad de acceso a los mecanizados es importante para el análisis de fugas de información
Total	A	Los datos de los mecanizados son realmente importantes para la correcta y continua producción de la empresa

Dependencias de activos inferiores	
Activo: Software de diseño	**¿Por qué?** Los mecanizados se generan empleando este software
Activo: NAS	**¿Por qué?** El NAS es el que almacena mecanizados y los deja a disposición de los empleados

- [K] Claves criptográficas

Código: K001	**Nombre:** Certificados empresa
Descripción: Certificados empleados por la empresa para realizar gestiones relacionadas con entidades publicas	
Propietario: Recursos humanos y Gerencia	**Responsable:** Gerente
Tipo: [info][sign][public_signature]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La no disponibilidad de los certificados de empresa puede afectar de forma negativa a las gestiones de la empresa
[I]	A	La modificación de los certificados de empresa podría afectar negativamente a las fabricaciones
[C]	MA	El uso no autorizado de los certificados de empresa podría poner en serios problemas al grupo empresarial
[A]	A	Es importante que los certificados sean reales para que el éxito del negocio tenga efecto
[T]	M	La trazabilidad de acceso a los certificados no es demasiado importante
Total	MA	Los certificados de empresa deben ser protegidos y usados con responsabilidad

Código: K002	**Nombre:** Claves ERP
Descripción: Claves necesarias para iniciar sesiones en el ERP Navision 2017.	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo:	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La no disponibilidad de las claves impediría el uso del ERP
[I]	A	La modificación de las claves del ERP las invalidaría
[C]	A	El uso de las claves por personas no autorizado podría llevar a una fuga de información
[A]	MA	Es importante que las claves sean reales para que el ERP las admita
[T]	MA	La trazabilidad en el uso de claves puede llevar a determinar accesos no autorizados
Total	MA	Los claves de acceso al ERP son necesarias para el funcionamiento del ERP

Dependencias de activos inferiores	
Activo: Servidor	**¿Por qué?** Las claves se almacenan en el servidor del ERP

- [S] Servicios

Código: S001	**Nombre:** Servicio de correo electrónico	
Descripción: Servicio de correo electrónico para los empleados de la empresa. Subcontratado a una empresa externa.		
Propietario: Responsable IT		**Responsable:** Empresa externa
Tipo: [email]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad del servicio de correo afecta directamente a las gestiones de la empresa.
[I]	A	La modificación de los correos afectaría directamente a negocio
[C]	MA	Es de extrema necesidad proteger la confidencialidad de los correos electrónicos
[A]	A	Es necesario asegurar que el servicio de correo siempre será el auténtico.
[T]	M	La trazabilidad de acceso al servicio de correo de cierta utilidad
Total	A	La clave debe protegerse para que no caiga en manos ajenas a la empresa

Código: S002	**Nombre:** Web de la empresa	
Descripción: Web de la empresa para poder anunciar la empresa y los servicios que ofrece en Internet. Gestionada por una empresa externa.		
Propietario: Responsable Comercial		**Responsable:** Empresa externa
Tipo: [www]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad de la web es necesaria para establecer relaciones comerciales
[I]	A	La modificación de la web podría afectar directamente a la imagen del negocio
[C]	MB	La información disponible es de dominio publico
[A]	M	Es de asegurar que la información será autentica
[T]	M	La trazabilidad de acceso a la web es de cierta utilidad
Total	M	La web es la fachada de la empresa al futuro cliente, por lo que se debe cuidar para dar una buena imagen.

Código: S003	**Nombre:** VPN
Descripción: Servicio de VPN ofrecido por la empresa para que los trabajadores puedan realizar teletrabajo.	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [telnet]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	M	La disponibilidad de la VPN puede afectar a empleados que necesiten conectarse en remoto
[I]	A	La modificación de la VPN inutilizaría la conexión
[C]	MA	El uso no autorizado de la VPN podría acarrear graves problemas a la empresa
[A]	A	Es necesario asegurarse de la autenticidad de la VPN
[T]	A	El registro de los acceso por VPN es de bastante utilidad
Total	A	La VPN debe protegerse para evitar accesos no deseados

Dependencias de activos inferiores	
Activo: Router	**¿Por qué?** El router ofrece el servicio de VPN para que se conecten a la red local
Activo: Fibra	**¿Por qué?** La VPN requiere de buen ancho de banda para asegurar las conexiones VPN necesarias

Código: S004	**Nombre:** Virtualización servidores
Descripción: El servicio de virtualización de servidores permite disponer de varios servidores lógicos en el mismo servidor físico	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo:	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad de los servidores virtualizados es vital para la actividad de la empresa
[I]	M	
[C]	M	
[A]	M	
[T]	A	La trazabilidad en el estado de los servidores virtualizados resulta necesaria para la comprobación del estado de estos servicios
Total	A	El servicio de virtualización de servidores resulta muy necesario para la empresa, por lo que es necesario asegurar su disponibilidad

Dependencias de activos inferiores	
Activo: Servidor	**¿Por qué?** El servicio se ejecuta en uno de los servidores, por lo que requiere los recursos del sistema

Código: S005	**Nombre:** Cortafuegos
Descripción: El servicio de cortafuegos actúa como una barrera entre internet u otras redes públicas y la red empresarial	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo:	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad del cortafuegos resulta muy util para evitar ataques externos
[I]	M	La integridad del cortafuegos debe ser considerada para evitar vulnerabilidades
[C]	-	
[A]	-	
[T]	M	La trazabilidad del cortafuegos debe registrarse para comprobar posibles manipulaciones
Total	M	El firewall resulta una de las protecciones más esenciales para proteger una red de ataques externos

Dependencias de activos inferiores	
Activo: Router	**¿Por qué?** El servicio de firewall actualmente se ejecuta en el router de la empresa

Código: S006	**Nombre:** DHCP
Descripción: Servicio que asigna automáticamente direcciones IP a los dispositivos que se conectan a la red.	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo:	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	M	La disponibilidad del servicio DHCP resulta útil para conectar dispositivos a la red inalámbrica únicamente.
[I]	M	La integridad del DHCP debe ser considerada para evitar vulnerabilidades
[C]	-	
[A]	-	
[T]	M	La trazabilidad del servicio DHCP debe registrarse para comprobar posibles manipulaciones
Total	A	El servicio DHCP resulta muy útil para conectar dispositivos a la red, aunque actualmente se encuentra configurado para solo ofrecer cierto rango de IPs

Dependencias de activos inferiores	
Activo: LAN	**¿Por qué?** El servicio DHCP escucha peticiones DHCP de las máquinas que se conectan a la red
Activo: Router	**¿Por qué?** El servicio de DHCP actualmente se ejecuta en el router de la empresa

Código: S007	**Nombre:** DNS
Descripción: Servicio de resolución de nombres que permite asignar nombres de dominio a direcciones de red	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo:	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	El servicio DNS tiene una gran importancia, por lo tanto es necesaria su completa disponibilidad
[I]	A	La integridad es útil tenerla considerada para evitar problemas de resolución de nombres
[C]	MB	
[A]	MA	Es necesario asegurar la autenticidad
[T]	B	Es útil conocer la trazabilidad por si hay cambios indebidos
Total	MA	El servicio DNS resulta indispensable tenerlo protegido para evitar posibles problemas de suplantación

Dependencias de activos inferiores	
Activo: Servicio de virtualización	**¿Por qué?** Este servicio se ejecuta en una máquina virtual

Código: S008	**Nombre:** Servidor impresión	
Descripción: Servicio que controla el sistema de impresiones de la empresa		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo:		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad del servicio es alta para permitir impresiones
[I]	B	La necesidad de asegurar la integridad del servicio es baja
[C]	B	La confidencialidad del servicio de impresión es baja
[A]	-	
[T]	B	La trazabilidad es útil para determinar que documentos y quien los ha impreso
Total	M	El servicio de impresión tiene una valoración media sobre el sistema
Dependencias de activos inferiores		
Activo: Servicio de virtualización		**¿Por qué?** Este servicio se ejecuta en una máquina virtual

Código: S009	**Nombre:** Active Directory
Descripción: Servicio de directorio que permite administrar usuarios, equipos y grupos	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [idm]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad del servicio es indispensable para que los empleados puedan realizar sus labores cotidianas
[I]	M	
[C]	A	La confidencialidad del servicio debe ser alta para impedir accesos no autorizados
[A]	M	
[T]	MA	La trazabilidad del servicio es indispensable para comprobar todos los cambios realizados
Total	MA	El servicio de Active Directory tiene una valoración muy alta, ya que toda la gestión de grupos y usuarios recae sobre su buena actuación

Dependencias de activos inferiores	
Activo: Servicio de virtualización	**¿Por qué?** Este servicio se ejecuta en una máquina virtual

Código: S010	**Nombre:** GPO
Descripción: Servicio de directivas de grupo que proporciona la gestión centralizada y configuración de sistemas operativos, aplicaciones y configuración de los usuarios	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [idm]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad del servicio es indispensable para que los empleados puedan realizar sus labores cotidianas
[I]	A	La integridad de las configuraciones debe ser preservada
[C]	M	Es interesante proteger las configuraciones de intrusos
[A]	B	
[T]	A	El necesario guardar la trazabilidad para comprobar siempre posibles cambios en las configuraciones
Total	MA	El servicio de GPO tiene una valoración muy alta, ya que toda la gestión de configuraciones recae sobre su buena actuación

Dependencias de activos inferiores	
Activo: Servicio de virtualización	**¿Por qué?** Este servicio se ejecuta en una máquina virtual

Código: S011	**Nombre:** DNS caché
Descripción: Servicio que guarda en caché aquellos datos que suelen ser consultados con frecuencia, con el objetivo de aliviar la carga de la red	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo:	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	M	La disponibilidad del servicio resulta útil pero no indispensable
[I]	M	La integridad del servicio resulta útil pero no indispensable
[C]	MB	No es necesario asegurar confidencialidad
[A]	A	La autenticidad debe asegurarse para impedir entradas DNS caché incorrectas
[T]	MB	No es necesaria una trazabilidad
Total	B	El servicio de DNS cache es útil para la empresa pero solo sirve para agilizar las peticiones web

Dependencias de activos inferiores	
Activo: Router	**¿Por qué?** El servicio de DNS caché actualmente se ejecuta en el router de la empresa

Código: S012	**Nombre:** QUEQUES
Descripción: Servicio que permite limitar el trafico externo y reducir el ancho de banda para aquellos dispositivos que superen la cuota	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo:	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	M	La disponibilidad del servicio resulta útil pero no indispensable
[I]	M	La integridad del servicio resulta útil pero no indispensable
[C]	B	No es necesario asegurar confidencialidad
[A]	-	
[T]	MB	No es necesaria una trazabilidad
Total	B	Este servicio es un complemento al tráfico de red

Dependencias de activos inferiores	
Activo: Router	**¿Por qué?** El servicio de QUEQUES actualmente se ejecuta en el router de la empresa

Código: S013	**Nombre:** WSUS
Descripción: Servicio que permite centralizar las actualizaciones para todas las máquinas de un dominio	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [email]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	M	La disponibilidad del servicio resulta útil pero no indispensable
[I]	M	La integridad del servicio resulta útil pero no indispensable
[C]	MB	No es necesario asegurar confidencialidad
[A]	M	Es útil comprobar la autenticidad de las actualizaciones
[T]	M	Es útil contar con la trazabilidad de las actualizaciones realizadas
Total	M	El servicio Wsus resulta útil para realizar la gestión de actualizaciones en el dominio

Dependencias de activos inferiores	
Activo: Servicio de virtualización	**¿Por qué?** Este servicio se ejecuta en una máquina virtual

Código: S014	**Nombre:** Servidor web interno
Descripción: Servidor web Apache + Tomcat que permite la ejecución de aplicaciones para uso interno.	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [www]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	Es necesario asegurar disponibilidad para que las aplicaciones internas funcionen correctamente
[I]	M	La integridad del servicio resulta útil pero no indispensable
[C]	MB	No es necesario asegurar confidencialidad
[A]	-	
[T]	M	Es útil contar con la trazabilidad de las acciones realizadas
Total	A	El servicio web se emplea mucho para las aplicaciones de la intranet empresarial

Dependencias de activos inferiores	
Activo: Servidor	**¿Por qué?** El servicio de Apache + Tomcat se ejecuta en el servidor

Código: S015	**Nombre:** Servidor ERP	
Descripción: Servicio servidor del ERP Navision 2017		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo:		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	Es completamente necesario asegurar disponibilidad para que los clientes ERP funcionen correctamente
[I]	MA	La integridad del servicio resulta indispensable
[C]	A	Es completamente necesario asegurar la confidencialidad de la información
[A]	MA	La autenticidad de la información es completamente necesaria asegurarla
[T]	MA	Es indispensable asegurar la trazabilidad para poder comprobar cualquier cambio realizado
Total	MA	El servidor ERP es indispensable para el buen desarrollo de la labor empresarial

Dependencias de activos inferiores	
Activo: Base de datos SQL Server	**¿Por qué?** El servidor ERP requiere un archivo de base de datos con el que trabajar

Código: S016	**Nombre:** PostgreSQL
Descripción: Servicio de base de datos PostgreSQL donde se alojan los datos del Gestor de Proyectos	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo:	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	Es necesario asegurar disponibilidad para que la aplicación del Gestor de Proyectos funcione correctamente
[I]	MA	La integridad del servicio resulta indispensable
[C]	A	Es completamente necesario asegurar la confidencialidad de la información
[A]	MA	La autenticidad de la información es completamente necesaria asegurarla
[T]	MA	Es indispensable asegurar la trazabilidad para poder comprobar cualquier cambio realizado
Total	MA	El servicio de PostgreSQL es necesario ser protegido para el correcto funcionamiento de la administración de la empresa

Dependencias de activos inferiores	
Activo: Base de datos PostgreSQL	**¿Por qué?** El servicio PostgreSQL requiere lectura y escritura de la base de datos PostgreSQL.

Código: S017	**Nombre:** Microsoft SQLServer
Descripción: Servicio de base de datos SQLServer donde se alojan los datos del ERP y de la aplicación de fabricación	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo:	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	Es completamente necesario asegurar disponibilidad para que los clientes ERP funcionen correctamente
[I]	MA	La integridad del servicio resulta indispensable
[C]	A	Es completamente necesario asegurar la confidencialidad de la información
[A]	MA	La autenticidad de la información es completamente necesaria asegurarla
[T]	MA	Es indispensable asegurar la trazabilidad para poder comprobar cualquier cambio realizado
Total	MA	El servicio ERP es indispensable para que la mayoría de las aplicaciones de la empresa funcionen correctamente

Dependencias de activos inferiores	
Activo: Base de datos SQL Server	**¿Por qué?** El servicio SQLServer requiere un archivo de base de datos con el que trabajar

- [SW] Software – Aplicaciones Informáticas

Código: SW001	**Nombre:** Paquete ofimático	
Descripción: Paquete de aplicaciones básicas para el trabajo de oficina		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [std][office]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad del software es importante para el trabajo del personal administrativo
[I]	-	
[C]	-	
[A]	-	
[T]	M	La trazabilidad de acceso a los documentos es importante para el análisis de fugas de información
Total	M	El paquete ofimático genera documentos a proteger

Código: SW002	**Nombre:** Cliente de correo
Descripción: Cliente de correo electrónico que se ejecuta de forma local en los PC	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [std][email_client]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad del cliente de correo es necesaria como forma de comunicación interna y externa de la empresa
[I]	A	La modificación de datos en los correos afectaría directamente a negocio
[C]	MA	La fuga de esta información afectaría directamente a negocio
[A]	MA	Es importante que los datos sean reales para que el éxito del negocio tenga efecto.
[T]	A	La trazabilidad de acceso a los correos es importante para el análisis de fugas de información
Total	A	El cliente de correo tiene vital importancia en las comunicaciones de la empresa

Dependencias de activos inferiores	
Activo: Servicio de correo electrónico	**¿Por qué?** El cliente de correo electrónico depende del servicio contratado de correo

Código: SW003	**Nombre:** Webmail	
Descripción: Cliente web de correo electrónico que se accede mediante el navegador web		
Propietario: Responsable IT		**Responsable:** Empresa externa
Tipo: [std][email_client]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	B	La disponibilidad del webmail no es muy necesaria, solo se usa en determinadas ocasiones puntuales
[I]	-	
[C]	-	
[A]	-	
[T]	-	
Total	B	El servicio de webmail se emplea únicamente cuando el cliente de correo electrónico no está disponible

Dependencias de activos inferiores	
Activo: Servicio de correo electrónico	**¿Por qué?** El cliente de correo electrónico depende del servicio contratado de correo
Activo: Navegador web	**¿Por qué?** Para acceder al web mail es necesario un navegador de internet

Código: SW004	**Nombre:** Navegador web	
Descripción: Navegador de Internet para poder consultar información en Internet		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [std][browser]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad del navegador web es necesaria para algunas tareas
[I]	M	La integridad del navegador afectaría levemente a negocio
[C]	M	Es necesario controlar la confidencialidad
[A]	M	Es importante que los datos sean reales para que el éxito del negocio tenga efecto.
[T]	M	La trazabilidad de acceso del navegador es importante para el análisis de fugas de información
Total	M	El navegador web requiere una leve configuración de seguridad
Dependencias de activos inferiores		
Activo: LAN		**¿Por qué?** Necesita que el equipo se encuentre conectado a una red

Código: SW005	**Nombre:** ERP (Microsoft Dynamics Navision 2017)
Descripción: Sistema de planificación de recursos empresariales. Estos programas se hacen cargo de distintas operaciones internas de una empresa, desde producción a distribución o incluso recursos humanos. Este en concreto es, Microsoft Dinamic Nav 2017	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [std]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	La disponibilidad del ERP es indispensable para la gestión de la producción de la empresa
[I]	MA	La modificación de datos de documentos afectaría directamente a negocio
[C]	MA	La fuga de esta información afectaría directamente a negocio
[A]	MA	Es importante que los datos sean reales para que el éxito del negocio tenga efecto.
[T]	MA	La trazabilidad de acceso a los documentos es importante para el análisis de fugas de información y errores
Total	EX	El ERP es una de las piezas de software indispensables para la buena gestión de la empresa, por lo que debe ser protegido en profundidad

Dependencias de activos inferiores	
Activo: Servicio servidor del ERP	**¿Por qué?** El cliente del ERP necesita conectarse a la máquina virtual donde se aloja el servicio servidor del ERP

Código: SW006	**Nombre:** Suite de diseño grafico	
Descripción: Diversos programas de diseño gráfico que permiten al departamento de diseño y diseño técnico diseñar los productos y realizar los mecanizados		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [std]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	Es importante disponer de la suite para el diseño y modificación de los productos
[I]	M	La integridad del programa es requerida para diseñar productos
[C]	A	La fuga de esta información afectaría directamente a negocio
[A]	M	La autenticidad es recomendada para el correcto diseño
[T]	A	La trazabilidad de acceso y modificación a los documentos es importante para el análisis de fugas de información
Total	A	La suite de diseño es una de las piezas más importantes a la hora de crear nuevos productos

Código: SW007	**Nombre:** Antivirus	
Descripción: Software antivirus que protege los equipos ante el malware y virus. ESET Nod32.		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [std][av]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad del antivirus es necesaria en todo momento para proteger cualquiera de las máquinas de la empresa de posibles focos de infección
[I]	MA	La modificación de las configuraciones del antivirus podría afectar negativamente
[C]	B	No trabaja con datos sensibles
[A]	M	
[T]	M	
Total	MA	El antivirus protege el sistema de malware y accesos no autorizados

Código: SW008	**Nombre:** Sistemas operativos
Descripción: La empresa dispone de diversos sistemas operativos para las diferentes maquinas con las que opera. Ubuntu Linux, Windows 10 y Windows XP para las terminales de las máquinas.	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [std][os]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	Es completamente necesario disponer de los sistemas operativos para poder trabajar
[I]	A	La integridad de los sistemas operativos es importante
[C]	A	Los sistemas operativos deben ofrecer protección ante las intrusiones
[A]	M	
[T]	A	Es muy util disponer de ficheros para comprobar la trazabilidad
Total	MA	Es necesario adoptar medidas de protección para corregir las vulnerabilidades que puedan aportar los sistemas operativos más antiguos.

Código: SW009	**Nombre:** Software de backups	
Descripción: Software para realizar y automatizar copias de seguridad. Backuppc y Veeam.		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [std][backup]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	Es necesario disponer del software de copias de seguridad para realizar las copias de seguridad cuando se requiera
[I]	A	Es necesario asegurar la integridad del sistema de copias de seguridad, para que las copias realizadas sean validas
[C]	M	
[A]	M	
[T]	M	
Total	A	El software de copias es un activo con gran valor

Código: SW010	**Nombre:** Software gestión Wifi
Descripción: Este software incluido con los dispositivos Wifi, permite comprobar el correcto funcionamiento de las antenas Wifi. En este caso en particular, se trata de Unifi.	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [std]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	B	La disponibilidad del software resulta útil en las ocasiones en las que se requiere.
[I]	B	No requiere control de integridad
[C]	B	No contiene datos sensibles
[A]	-	
[T]	-	
Total	B	El software resulta útil para resolver incidencias relacionadas con las antenas Wifi y realizar algunas configuraciones

Dependencias de activos inferiores	
Activo: Servidor virtual	**¿Por qué?** Este software se ejecuta en uno de los servidores virtuales

Código: SW011	**Nombre:** Software de fabricación
Descripción: Este software desarrollado por la propia empresa permite a los operarios indicar los tiempos requeridos en los procesos de fabricación	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [prp]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad del software de fabricación es necesaria para la gestión de la producción en tiempo real
[I]	M	No requiere control de integridad
[C]	B	No contiene datos sensibles
[A]	M	La autenticidad se valora positivamente
[T]	A	La trazabilidad permite comprobar que usuarios han registrado determinadas acciones
Total	A	El software de fabricación resulta realmente util para controlar el proceso de fabricación

Dependencias de activos inferiores	
Activo: Servicio Apache+Tomcat	**¿Por qué?** Este aplicación se lanza en el servidor propio de la red interna

Código: SW012	**Nombre:** Software de gestión de proyectos	
Descripción:		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [prp]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad de este software resulta indispensable para que gerencia realice las mayoría de sus tareas
[I]	A	La integridad de los datos de este programa debe ser alta
[C]	M	Debe restringirse ciertos accesos a la información
[A]	M	
[T]	A	La trazabilidad es necesaria para comprobar quien y cuando realiza acciones no deseadas
Total	MA	El software de gestión de proyectos es una de las piezas claves para la gestión de la actividad empresarial

Dependencias de activos inferiores	
Activo: Base de datos ERP	**¿Por qué?** El software de gestión de proyectos necesita leer información generada desde el ERP

Código: SW013	**Nombre:** Wiki interna documentación
Descripción: El departamento de Informática cuenta con una wiki donde dispone de bastantes procedimientos ante casos específicos como instalaciones, realización de tareas…	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [std]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	B	La disponibilidad de la wiki puede resultar útil para determinadas consultas
[I]	B	No requiere control de integridad
[C]	B	No contiene datos sensibles
[A]	-	
[T]	B	La wiki dispone de una forma de asegurar la trazabilidad
Total	B	La wiki es una herramienta que permite a los empleados del departamento IT disponer de ciertos procedimientos compartidos

Dependencias de activos inferiores	
Activo: Servidor	**¿Por qué?** La wiki se ejecuta sobre el servidor

Código: SW014	**Nombre:** Software control inventario informático
Descripción: El software de control de inventario informático GLPI permite al departamento de informática tener constancia de los activos disponibles, su localización y estado.	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [std]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad resulta de suma importancia
[I]	M	La integridad de los datos no se controla
[C]	A	La confidencialidad se protege con contraseña
[A]	-	
[T]	M	Se dispone de un registro de la trazabilidad
Total	A	Este software resulta un activo de bastante valor para llevar un control sobre los activos de la empresa

Dependencias de activos inferiores	
Activo: Servidor	**¿Por qué?** Este software se ejecuta en uno de los servidores

- [HW] Hardware – Equipamiento Informático

Código: HW001	**Nombre:** Ordenadores oficina (40)	
Descripción: Ordenadores estándar de oficina		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [pc]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	B	Estos ordenadores son fáciles de reemplazar
[I]	M	La integridad corresponde a un valor normal
[C]	M	El acceso no autorizado solo podría afectar a los datos de usuario
[A]	-	
[T]	-	
Total	M	Los ordenadores de oficina son un bien fácil de reemplazar

Código: HW002	**Nombre:** Ordenadores portátiles (15)
Descripción: Ordenadores portátiles preparados para que los comerciales puedan conectarse a la red empresarial empleando VPN y las credenciales	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [mobile]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	B	Estos ordenadores son fáciles de reemplazar
[I]	M	La integridad corresponde a un valor normal
[C]	M	El acceso no autorizado solo podría afectar a los datos de usuario
[A]		
[T]		
Total	M	Los ordenadores portátiles son un bien fácil de reemplazar

Dependencias de activos inferiores	
Activo: VPN	**¿Por qué?** Los ordenadores portátiles solo pueden conectarse desde el exterior a la red empresarial mediante VPN

Código: HW003	**Nombre:** Ordenadores diseño (15)
Descripción: Ordenadores equipados con una gráfica potente preparados para el diseño por ordenador de componentes	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [mid]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	Estos ordenadores al ser tan específicos y costosos, son un bien algo más difícil de reemplazar que uno de oficina común
[I]	M	La integridad corresponde a un valor normal
[C]	M	El acceso no autorizado solo podría afectar a los datos de usuario
[A]	-	
[T]	-	
Total	A	Los ordenadores de diseño son un bien muy valioso

Código: HW004	**Nombre:** Tabletas producción (20)	
Descripción: Tabletas donde los operarios ficharan sus trabajos realizados		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [mobile]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	B	Estas tabletas son muy fáciles de reemplazar y de configurar
[I]	M	La integridad corresponde a un valor normal
[C]	MB	Las tabletas tienen el acceso a la red completamente limitado
[A]	-	
[T]	-	
Total	B	Las tabletas están preparadas y configuradas únicamente para que los operarios realicen los fichajes y puedan consultar planos
Dependencias de activos inferiores		
Activo: Red Wifi		**¿Por qué?** No disponen de puertos Ethernet

Código: HW005	**Nombre:** Ordenadores producción (6)
Descripción: Ordenadores de sobremesa antiguos empleados en la producción para la ejecución de algunos programas de las máquinas de la producción, por lo que algunos de ellos requieren el uso de sistemas operativos obsoletos	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [pc]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	B	Estos ordenadores son sencillos de reemplazar
[I]	M	La integridad corresponde a un valor normal
[C]	M	El acceso no autorizado solo podría afectar a los datos contenidos en el equipo
[A]	-	
[T]	-	
Total	B	Los ordenadores de producción son un bien fácil de reemplazar, aunque hay que tener cuidado con posibles vulnerabilidades de los SO

Código: HW006	**Nombre:** NAS (2)	
Descripción: Servidores de archivos		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [mid]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	La disponibilidad del NAS debe ser ininterrumpida
[I]	MA	La integridad de los datos del NAS es muy preciada
[C]	MA	El acceso no autorizado afectara a la empresa
[A]	-	
[T]	-	
Total	MA	El NAS carga con todo el almacenamiento de datos de la empresa

Código: HW007	**Nombre:** Router (1)	
Descripción: Router que permiten la conexión de la red empresarial con Internet y entre las distintas naves industriales		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [network][router]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad del router es esencial para las comunicaciones de la empresa con el exterior y entre las distintas naves
[I]	MA	La integridad del router es de gran importancia
[C]	MA	El acceso no autorizado afectará en gran medida a la empresa
[A]		
[T]		
Total	MA	El router debe ser uno de los bienes más protegidos

Código: HW008	**Nombre:** Impresoras (20)	
Descripción: Impresoras standard de oficina. Contratadas a un servicio externo.		
Propietario: Gerente		**Responsable:** Empresa externa
Tipo: [peripheral][print]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	M	Estas máquinas por lo general son fáciles de reemplazar
[I]	M	La integridad corresponde a un valor normal
[C]	B	El acceso no autorizado solo podría afectar a la configuración local de la impresora
[A]	-	
[T]	B	El registro de trazabilidad permite ver quién y que se ha impreso
Total	M	Las impresoras de oficina son un bien fácil de reemplazar
Dependencias de activos inferiores		
Activo: Servicio de impresión		**¿Por qué?** Las impresoras necesitan conectarse al servicio para estar disponibles para la red empresarial

Código: HW009	**Nombre:** Servidores físicos (3)
Descripción: Servidores de virtualización, dominio, red, datos y aplicaciones de la empresa	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [host]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	La disponibilidad del servidor es fundamental para la empresa
[I]	EX	La integridad del servidor es fundamental para la empresa
[C]	EX	El acceso no autorizado podría hacer perder a la empresa sus datos
[A]	MA	Es necesario que toda comunicación con ellos sea autenticada
[T]	MA	Es necesario mantener un registro de trazabilidad de los cambios de los servidores
Total	EX	Los servidores como centros neurálgicos de la informática de la empresa deben ser fuertemente protegidos

Dependencias de activos inferiores	
Activo: CPD	**¿Por qué?** Estos equipos deben ser resguardados en un lugar completamente inaccesible y seguro

Código: HW010	**Nombre:** Servidores virtualizados (12)
Descripción: Servidores virtualizados donde se ejecutan la mayor parte de los servicios y aplicaciones de la empresa	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [vhost]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad de los servidores virtualizados debe ser alta por la gran cantidad de servicios que alojan
[I]	A	La integridad de los servidores debe ser alta
[C]	MA	El acceso no autorizado podría hacer perder a la empresa algunos de sus datos
[A]	MA	Es necesario que toda comunicación con ellos sea autenticada
[T]	A	Se recomienda mantener un registro de trazabilidad de los cambios de las maquinas virtuales
Total	MA	Los servidores virtualizados son necesarios para el buen hacer del negocio

Dependencias de activos inferiores	
Activo: Servidor	**¿Por qué?** Los servidores virtualizados consumen los recursos del servidor donde se alojan

Código: HW011	**Nombre:** Switch (12)
Descripción: Conmutadores de red que dan acceso a una gran cantidad de dispositivos a la red local	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [network][switch]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad debe ser muy elevada para evitar problemas de la red
[I]	A	La integridad debe ser elevada para evitar problemas de la red
[C]	A	El acceso no autorizado podría dar problemas en las comunicaciones
[A]	-	
[T]	A	Es beneficioso contar con un servicio de LOG
Total	A	Los switches son un bien necesario para la conexión de diferentes máquinas a la red

Dependencias de activos inferiores	
Activo: Router	**¿Por qué?** Los switches deben conectarse al router para proveer de la conexión de red entre sedes y con la red externa

Código: HW012	**Nombre:** Antenas enlace sedes (4)
Descripción: Antenas bidireccionales que permiten comunicar las diferentes sedes de la empresa	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [network]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	Es completamente indispensable mantener las conexiones activas entre diferentes localizaciones de la empresa
[I]	MA	La integridad debe permanecer asegurada
[C]	MA	La confidencialidad de los datos debe ser protegida de escuchadores de frecuencias
[A]	EX	La autenticidad de las conexiones debe protegerse con comprobaciones
[T]		
Total	EX	Las antenas de enlace entre sedes son la única forma de conexión entre algunas de las localizaciones propiedad de la empresa

Código: HW013	**Nombre:** Antenas Wifi (12)
Descripción: Pequeñas antenas Wifi que permiten proveer de Wifi a una zona muy reducida de la empresa	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [network]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad de las antenas Wifi debe ser alta
[I]	M	La integridad afecta de manera moderada a las comunicaciones
[C]	M	La confidencialidad es protegida de manera estándar en la Wifi
[A]	-	
[T]	-	
Total	A	Las antenas Wifi proveen de conexión a aquellas maquinas ajenas a la empresa y a aquellas que no disponen de puertos Ethernet de conexión

Dependencias de activos inferiores	
Activo: DHCP	**¿Por qué?** La antenas dependen del DHCP para saber que IPs pueden ofrecer o no

Código: HW014	**Nombre:** Mini-switch (20)
Descripción: Pequeños switch de soporte que proveen de wifi a aquellas zonas de la empresa que no disponen de una infraestructura de red preparada adecuadamente	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [network][switch]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad debe ser muy elevada para evitar problemas de la red con las máquinas que dependan del mini-switch
[I]	A	La integridad debe ser elevada para evitar problemas de la red
[C]	MA	Una máquina externa a la organización puede usarla para conectarse a la organización de forma peligrosa
[A]	-	
[T]	A	Es beneficioso contar con un servicio de LOG
Total	MA	Los mini-switches al igual que los switch normales, proveen de conexión de red a las diferentes máquinas. Pero sus medidas de seguridad son bastante ineficientes, pudiendo provocar bucles en la red, por lo que se deben de proteger mejor.

Dependencias de activos inferiores	
Activo: Router	**¿Por qué?** Los switches deben conectarse al router para proveer de la conexión de red entre sedes y con la red externa

Código: HW015	**Nombre:** Impresoras térmicas (20)
Descripción:	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [peripheral][print]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	M	Cada puesto de trabajo dispone de su impresora, por lo que la disponibilidad es alta
[I]	M	La integridad corresponde a un valor normal
[C]	MB	La información impresa no requiere ser protegida
[A]	-	
[T]	MB	No se requiere trazabilidad de impresiones
Total	MB	Las impresoras térmicas solo sirven la función de imprimir tickets para reflejar en los pallets la trazabilidad del producto

Dependencias de activos inferiores	
Activo: Servicio de impresión	**¿Por qué?** Las impresoras requieren de este servicio para manejar sus colas de impresión

Código: HW016	**Nombre:** Terminales (20)
Descripción: Los terminales son aquellas interfaces o paneles que permiten a los operarios controlar las máquinas de la producción	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [pc]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	Las terminales deben de estar disponibles para permitir a los operarios trabajar con las máquinas dedicadas a la producción
[I]	A	La integridad debe ser protegida
[C]	MB	No se trabaja con datos sensibles
[A]	-	
[T]	A	La trazabilidad de las acciones en los terminales debe ser registrada
Total	A	Los terminales requieren una buena protección para asegurar el buen y correcto funcionamiento de la maquinaria

Código: HW017	**Nombre:** Autómatas (20)	
Descripción: Máquina automática programable capaz de realizar determinadas operaciones de manera autónoma. Sirven para asistir al operario con la fabricación.		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [mobile]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad de los autómatas afecta a la maquinaria industrial y por lo tanto a la actividad de negocio
[I]	A	La integridad debe ser asegurada para impedir un comportamiento no deseado
[C]	MB	No se trabaja con datos sensibles
[A]	-	
[T]	A	Es importante que conserven un registro de las acciones
Total	A	Los autómatas como una pieza necesaria de la maquinaria industrial deben ser protegidas y aseguradas

Código: HW018	**Nombre:** Servidor de copias
Descripción: El servidor de copias asiste a la realización de las copias diarias y semanales de la información contenida en los distintos servidores	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [backup]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad debe ser alta ya que se debe usar varias veces al día
[I]	A	La integridad es indispensable para que las copias no sean erroneas
[C]	A	La confidencialidad debe ser alta para impedir fugas
[A]	A	La autenticidad de las copias debe ser asegurada
[T]	A	La trazabilidad debe ser alta para conocer que copias se han realizado correctamente o no
Total	A	El servidor de copias se dedica a la realización de las copias diarias y semanales, por lo que se debe asegurar su buen funcionamiento

- [COM] Redes de comunicaciones

Código: COM001	**Nombre:** Red local	
Descripción: Red local que conecta servidor, equipos, impresoras y da conectividad a otros servicios		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [LAN]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	La no disponibilidad de la red local afectaría negativamente a toda la empresa.
[I]	MA	Es importante que los datos conserven su integridad para que el éxito del negocio tenga efecto.
[C]	MA	La fuga de esta información afectaría directamente a negocio
[A]	A	Es importante que los datos sean reales para que el éxito del negocio tenga efecto.
[T]	A	La trazabilidad de acceso a la red local es importante para el análisis de fugas de información y accesos no deseados
Total	EX	El acceso a la red local debe ser restringido únicamente a los equipos confiables y se debe añadir monitorización
Dependencias de activos inferiores		
Activo: Router		**¿Por qué?** Requieren la configuración de encaminamiento del router
Activo: Switch		**¿Por qué?** Requieren la configuración del switch para poder conectarse todas las maquinas a la LAN

Código: COM002	**Nombre:** ADSL	
Descripción: Dispositivo USB que permite ofrecer una conexión a Internet al dispositivo al que se conecte		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [ADSL]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MB	Se utiliza solo en ocasiones de emergencia
[I]	-	
[C]	B	No ofrece demasiada protección ante posibles escuchas de la señal
[A]	-	
[T]	-	
Total	B	Aunque en el pasado se utilizaba bastante esta forma de conexión, actualmente solo se emplea con los ordenadores portatiles

Código: COM003	**Nombre:** Servicio telefonía
Descripción: Red de telefonía móvil que permite a la empresa estar en contacto telefónico	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [PSTN][mobile]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	Es una de las principales herramientas entre el personal de la empresa y las comunicaciones externas, por lo que su disponibilidad es esencial
[I]	A	La integridad de las comunicaciones es importante
[C]	A	La confidencialidad de las llamadas es necesaria
[A]	A	La autenticidad de las comunicaciones debe asegurarse
[T]	B	La trazabilidad de las llamadas resulta de ayuda
Total	MA	La red telefónica es uno de los bienes más empleados en día a día de las comunicaciones de la empresa

Código: COM004	**Nombre:** Red Wifi
Descripción: Red inalámbrica que permite el acceso de dispositivos móviles	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [wifi]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad debe ser alta para la red wifi empresarial y para la red de clientes
[I]	M	La integridad puede afectar a la calidad de la conexión
[C]	M	La confidencialidad tiene que protegerse
[A]	-	
[T]	-	
Total	M	La red Wifi en parte actúa como complemento de la red cableada, aunque algunas de las máquinas dependen exclusivamente de ella

Dependencias de activos inferiores	
Activo: Antenas Wifi	**¿Por qué?** Las antenas Wifi son las que emiten y reciben las señales Wifi que permiten a los dispositivos conectarse a la red
Activo: Router	**¿Por qué?** El router ofrece ciertas direcciones IP dedicadas a las conexiones Wifi

Código: COM005	**Nombre:** Fibra
Descripción: Enlace principal de comunicaciones digitales que permite la conexión del grupo empresarial con Internet	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [ISDN]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad de la red externa es un bien muy necesario para las comunicaciones de la empresa
[I]	A	Es importante mantener la integridad del servicio
[C]	MA	Es necesario proteger el acceso de internet de la empresa
[A]	A	Es importante que los datos sean reales para que el éxito del negocio tenga efecto
[T]	A	La trazabilidad de acceso a la red externa es deseable controlarlo
Total	MA	El acceso a la red externa es un bien muy preciado, ya que permite la comunicación con clientes, proveedores…

Dependencias de activos inferiores	
Activo: Router	**¿Por qué?** El router sirve de nexo entre la red externa y la LAN interna

Código: COM006	**Nombre:** Fibra oscura	
Descripción: Esta fibra dedicada actúa como punto a punto entre sedes de la empresa		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [pp]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad del enlace debe ser muy alta para que las sedes se encuentren comunicadas
[I]	MA	La integridad de datos debe asegurarse con el proveedor
[C]	-	
[A]	-	
[T]	-	
Total	MA	El enlace de fibra oscura es bien muy apreciado que permite conectar las sedes entre sí como si de una misma LAN se tratase
Dependencias de activos inferiores		
Activo: Router		**¿Por qué?** El router sirve de nexo entre el enlace de fibra y la LAN interna

Código: COM007	**Nombre:** Enlaces antenas
Descripción: Este enlace por antena actúa como punto a punto entre diferentes sedes de la empresa	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [pp]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	La disponibilidad del enlace debe ser muy alta para que las sedes principales se encuentren comunicadas
[I]	MA	La integridad debe protegerse entre las antenas
[C]	MA	La confidencialidad afectará a las posibles escuchas de información
[A]	MA	Es necesario mantener la autenticidad de los datos
[T]	A	Asegurar una trazabilidad del estado de las antenas nos permitirá prevenir algunos problemas
Total	EX	El enlace de antenas es uno de los bienes más preciados ya que permite conectar las sedes principales entre sí como si de una misma LAN se tratase

Dependencias de activos inferiores	
Activo: Router	**¿Por qué?** El router sirve de nexo entre el enlace de antena y la LAN interna

- [Media] Soportes de información

Código: MEDIA001	**Nombre:** Discos duros extraíbles	
Descripción: Soporte almacenamiento externo tipo disco SSD encriptado empleado para guardar backups		
Propietario: Responsable IT	**Responsable:** Gerente	
Tipo: [electronic] [disk]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad de los discos podría llevar a un retraso en la creación de backups
[I]	MA	La modificación de datos de los discos duros de backups podrían afectar directamente al negocio
[C]	EX	La fuga de esta información afectaría directamente a negocio
[A]	-	
[T]	-	
Total	MA	Los discos duros deben ser almacenados en un sitio seguro ya que aunque la información se encuentre encriptada, dispone de información confidencial

Código: MEDIA002	**Nombre:** Blue-Ray
Descripción: Soporte de almacenamiento Blue-Ray Disk usado para guardar copias de seguridad trimestrales de la información	
Propietario: Responsable IT	**Responsable:** Gerente
Tipo: [electronic] [dvd]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	B	Los discos se utilizan en muy raras ocasiones para cosas puntuales
[I]	M	La modificación de datos de los discos duros de backups podrían afectar de forma moderada al negocio
[C]	A	La fuga de esta información podría afectar al negocio
[A]	-	
[T]	-	
Total	A	Los discos contienen información encriptada, pero aun así deben ser protegidos

- [AUX] Equipamiento auxiliar

Código: AUX001	**Nombre:** Lector de huellas dactilares	
Descripción: Sensor de huellas dactilares usados para marcar el fichaje de los operarios. Sistema actualmente en desuso.		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo:		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MB	Actualmente no se usa, pues fichan directamente en la aplicación
[I]	-	
[C]	-	
[A]	-	
[T]	B	Ofrece un registro de entradas y salidas del personal
Total	MB	Actualmente su valor es mínimo para negocio
Dependencias de activos inferiores		
Activo: LAN		**¿Por qué?** Requiere de la red local para el almacenamiento de la información

Código: AUX002	**Nombre:** Cámaras de video seguridad	
Descripción: Cámaras de seguridad para vigilar los accesos a las naves		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo:		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad debe ser alta para no dejar ningún momento del día sin grabación registrada
[I]	A	La integridad de las grabaciones podrían afectar directamente al negocio
[C]	A	Es necesario proteger la confidencialidad de las grabaciones
[A]	-	
[T]	-	
Total	A	Las grabaciones deben ser protegidas para evitar manipulaciones

Código: AUX003	**Nombre:** Sai	
Descripción: Sistema de alimentación ininterrumpida. Permiten asegurar la disponibilidad en los servidores, pcs y dispositivos de comunicaciones ante caídas de tensión.		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [ups]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	M	La disponibilidad de los SAI es necesaria para asegurar que un corte de luz no apague los sistemas
[I]	A	La integridad de los SAI es necesaria para asegurar el correcto funcionamiento de los SAI
[C]	-	
[A]	-	
[T]	-	
Total	M	Los SAI pueden ayudar a proteger el sistema ante un corte de luz.

Código: AUX004	**Nombre:** Equipo de climatización	
Descripción: Equipos de climatización destinados a refrigerar el CPD y evitar recalentamientos de las máquinas esenciales de la infraestructura informática		
Propietario: Responsable IT		**Responsable:** Gerente
Tipo: [ac]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad del sistema de climatización debe ser ininterrumpida
[I]	MA	La integridad debe revisarse cada cierto tiempo
[C]	-	
[A]	-	
[T]	-	
Total	MA	La correcta climatización es esencial para el buen funcionamiento de las maquinas principales de la infraestructura informática

- [L] Instalaciones

Código: L001	**Nombre:** Nave principal	
Descripción: Sede principal de la empresa donde se encuentra gerencia, el CPD y la mayor parte de las oficinas		
Propietario: Gerente		**Responsable:** Gerente
Tipo: [building]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	La disponibilidad del edificio es completamente necesaria
[I]	MA	La integridad de la sede afecta directamente al negocio
[C]	MA	El acceso no autorizado afectaría directamente a negocio
[A]	-	
[T]	-	
Total	MA	Es necesario controlar el acceso al edificio.

Código: L002	**Nombre:** Almacén principal	
Descripción: Almacén principal de la empresa donde se realiza parte de la producción y se realizan los envíos		
Propietario: Gerente	**Responsable:** Gerente	
Tipo: [building]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	La disponibilidad del edificio es completamente necesaria
[I]	MA	La integridad de la sede afecta directamente al negocio
[C]	MA	El acceso no autorizado afectaría directamente a negocio
[A]	-	
[T]	-	
Total	MA	Es necesario controlar el acceso al edificio.

Código: L003	**Nombre:** Nave secundaria	
Descripción: Nave industrial de apoyo donde se realiza parte de la producción		
Propietario: Gerente		**Responsable:** Gerente
Tipo: [building]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad del edificio es temporal
[I]	M	La integridad de la sede afecta directamente al negocio
[C]	MA	El acceso no autorizado afectaría directamente a negocio
[A]	-	
[T]	-	
Total	M	Se recomienda controlar el acceso al edificio.

Código: L004	**Nombre:** Almacén secundario
Descripción: almacén de apoyo que ofrece soporte al almacenamiento y procesos que no pueden ser realizados en el principal	
Propietario: Gerente	**Responsable:** Gerente
Tipo: [building]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	A	La disponibilidad del edificio es temporal
[I]	M	La integridad de la sede afecta directamente al negocio
[C]	MA	El acceso no autorizado afectaría directamente a negocio
[A]	-	
[T]	-	
Total	M	Se recomienda controlar el acceso al edificio.

Código: L005	**Nombre:** CPD
Descripción: Centro de Procesamiento de Datos de la empresa, donde se encuentran los servidores de la empresa	
Propietario: Gerente	**Responsable:** Gerente
Tipo: [local]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	La disponibilidad es absolutamente necesaria
[I]	EX	La integridad del CPD afecta directamente al negocio
[C]	EX	El acceso no autorizado afectaría de manera muy negativa a negocio
[A]	-	
[T]	MA	Es necesario configurar algún tipo de trazabilidad al acceso al CPD
Total	EX	Es necesario controlar el acceso al CPD.

- [P] Personal

Código: P001	**Nombre:** Gerencia	
Descripción: Departamento de dirección de la empresa		
Propietario: Gerente		**Responsable:** Gerente
Tipo: [ui]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	EX	La disponibilidad de la gerencia es necesaria para el negocio
[I]	MA	La integridad de los empleados afectaría directamente al negocio
[C]	EX	La fuga de información afectaría directamente a negocio
[A]	-	
[T]	-	
Total	EX	La gerencia es absolutamente necesaria para negocio

Código: P002	**Nombre:** Oficina
Descripción: Empleados de la empresa de cada uno de los departamentos de administración y diseño que trabajan desde la propia empresa	
Propietario: Gerente	**Responsable:** Gerente
Tipo: [ui]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	M	La disponibilidad de los empleados puede acomodarse a la demanda
[I]	M	La integridad de los empleados afectaría moderadamente al negocio
[C]	MA	La fuga de información afectaría directamente a negocio
[A]	-	
[T]	-	
Total	MA	Los empleados deben ser conscientes de la importancia de la seguridad

Código: P003	**Nombre:** Comerciales
Descripción: Empleados de la empresa que viajan ofreciendo los productos de la empresa a otras empresas interesadas.	
Propietario: Gerente	**Responsable:** Gerente
Tipo: [ue]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad de la gerencia es necesaria para el negocio
[I]	M	La integridad de los empleados afectaría directamente al negocio
[C]	MA	La fuga de información afectaría directamente a negocio
[A]	-	
[T]	-	
Total	M	Los comerciales deben de asegurarse de no usar redes inseguras.

Código: P004	**Nombre:** Servicio informática
Descripción: Empleados de la empresa que administran todo el servicio de informática, redes, redes, seguridad.	
Propietario: Gerente	**Responsable:** Gerente
Tipo: [adm][com][dba][sec][des]	

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	MA	La disponibilidad del servicio de informática es necesaria para el día a día del negocio
[I]	MA	La integridad de los empleados afectaría directamente al negocio
[C]	EX	La fuga de información afectaría directamente a negocio
[A]	-	
[T]	-	
Total	MA	Los empleados de informática deben ser supervisados por un responsable.

Código: P005	**Nombre:** Operario	
Descripción: Personal encargado de las tareas de producción en fabrica		
Propietario: Gerente		**Responsable:** Gerente
Tipo: [op]		

Valoración		
Dimensión	**Valor**	**Justificación**
[D]	B	La disponibilidad de los operarios es reemplazable
[I]	B	La integridad de los operarios no afectaría al negocio
[C]	B	La fuga de información por parte de los operarios afectaría de forma moderada al negocio
[A]	-	
[T]	-	
Total	B	Los operarios no deben ser encomendados con información relevante para la empresa.